EMPLOYEES' SENSITIVE INFORMATION DISCLOSURE BEHAVIOR IN ENTERPRISE INFORMATION SYSTEMS

TECHNISCHE UNIVERSITÄT DARMSTADT

Vom Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt

genehmigte
Dissertation

von
Sarah Anna Elisabeth Träutlein (M. Sc.)
aus Heidelberg

Zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter:	Prof. Dr. Peter Buxmann
Zweitgutachter:	Prof. Dr. Alexander Benlian
Tag der Einreichung:	01.03.2017
Tag der mündlichen Prüfung:	10.10.2017

Darmstadt 2017
D17

Wissenschaftlicher Werdegang von Frau Sarah Träutlein

2014 – 2017	Dissertation zur Erlangung des akademischen Grades „Doctor rerum politicarum“, Technische Universität Darmstadt Thema der Dissertation: *„Employees‘ Sensitive Information Disclosure Behavior in Enterprise Information Systems“*
2011 – 2013	Master of Science in Wirtschaftsinformatik, Universität Mannheim Thema der Masterarbeit: *“How does Scrum influence the empowerment of software development teams.”*
2008 – 2011	Bachelor of Science in Wirtschaftsinformatik, Universität Mannheim

German Summary of the Dissertation

In der Dissertation "Employees' Sensitive Information Disclosure Behavior in Enterprise Information Systems" wurde die Bereitschaft von Mitarbeitern[1] untersucht, private und persönliche Informationen in Unternehmenssoftware preiszugeben.

Mehr und mehr werden soziale Intranetzwerke, Smartphone Apps, HR Analysetools, oder Personal-Feedbacksysteme, in Unternehmen eingeführt, um Mitarbeitern zu ermöglichen an ihrem Arbeitsplatz effizienter zu sein und ihr Verhalten, insbesondere ihre Bedürfnisse besser zu verstehen. Die Arbeit zeigt auf, dass die Einführung solcher Unternehmenssoftware nicht nur zu einer Steigerung der Arbeitsleistung und einer umfassenderen Betrachtung des eigenen Arbeitsverhaltens führt, sondern auch einen gegenteiligen Effekt erzielen kann. Etwa, dass die Arbeitnehmer das Gefühl haben, die Daten könnten missbräuchlich gegen sie verwendet werden. Rückbeziehend auf die Ergebnisse diskutiert die Arbeit konkret diese „Perceived Information-Based Vulnerability" (PIBV)[2] der Mitarbeiter. Ferner untersucht die Dissertation die daraus resultierende Bereitschaft sensitive Informationen preiszugeben oder gegenüber dem System Strategien des Widerstandes zu entwickeln. Aus den Erkenntnissen konnten darüber hinaus Empfehlungen für eine erfolgreiche Implementierung von Unternehmenssoftware abgeleitet werden.

Methodisch gesehen wurde als theoretische Fundierung der Arbeit eine ausführliche Literaturrecherche zum Forschungsfeld „Preisgabe sensitiver Informationen in Informationssystemen", mit Fokus auf E-Commerce Plattformen und soziale Netzwerke, wie etwa Facebook, angestellt. Daraus abgeleitet erfolgte eine explorative, qualitative Studie die in weiterer Folge zur Entwicklung eines Ursache-Wirkungs-Modells führte. Dieses wurde in einer weiteren Phase der Arbeit quantitativ evaluiert. Um das Modell auf die praktische Anwendbarkeit zu überprüfen erfolgte in einer abschließenden Phase eine quantitative Praxisstudie. In weiterer Folge werden nun die einzelnen Phasen der Arbeit im Detail erläutert.

Literaturrecherche

Wie die Recherchen ergaben, existieren kaum systematische Analysen zum Thema *Preisgabe sensitiver Informationen von Mitarbeitern in Unternehmenssoftware*. Daher war es nötig das zu analysierende Begriffsfeld weiter zu fassen. Somit wurden auch Erkenntnisse aus dem Forschungsbereich *allgemeine Preisgabe sensitiver Informationen in Informationssystemen* zur Analyse herangezogen. Die Untersuchung lieferte wertvolle Erkenntnisse hinsichtlich der Preisgabe sensitiver Informationen von Softwarenutzern. Darüber hinaus konnten erfolgsversprechende Konzepte bzw. identifizierte Einflussfaktoren für eine solche Preisgabe aufgezeigt werden, zum Beispiel in sozialen Netzwerken, auf E-Commerce Webseiten oder auch in Gesundheitsportalen. Die Privacy-Forschung kristallisierte sich als leitenden Forschungsstrang

[1] Mit Mitarbeiter sind hier männliche, als auch weibliche Mitarbeiter gemeint. Zum simplifizieren des Textes wird auf das weibliche Geschlecht im Fließtext verzichtet.

[2] Entspricht im Deutschen der wahrgenommenen Verletzlichkeit durch Preisgabe von Informationen

heraus, insbesondere die Privacy-Calculus-Theorie (Dinev und Hart 2006) wurde als grundlegende Theorie für diese Arbeit identifiziert.

Qualitative Studie

In semi-strukturierten Experteninterviews wurden die Auswirkungen der identifizierten Einflussfaktoren aus der Privacy-Literatur und mögliche weitere organisatorische Faktoren untersucht. Hierbei wurde im Besonderen die Wahrnehmung sozialer Intranetzwerke (Enterprise Social Systems) durch Mitarbeiter und deren Preisgabeverhalten erforscht.

Die Inhaltsanalyse der Interviews ergab, dass Mitarbeiter es als gefährlich erachten, sensitive Informationen preiszugeben, da dies das Potential eines Missbrauchs durch den Arbeitgeber in sich bergen. Als Reaktionsverhalten darauf konnten mehrere mögliche Szenarien identifiziert werden:

- Verweigerung der Informationspreisgabe
- Falsche Informationspreisgabe
- Widerstand gegen die Informationspreisgabe bzw. die Software allgemein

Aus den Rückmeldungen konnte ebenfalls abgeleitet werden, dass Mitarbeiter die Einführung neuer Software häufig mit vermeintlichen (opportunistischen) Beweggründen eines Unternehmens verbinden. Konkret beeinflusst wird diese Wahrnehmung durch die Eigenschaften der Softwarelösung, den wahrgenommenen Mehrwert und das Vertrauensverhältnis und die Beziehung zum Arbeitgeber. Theoretisch gestützt werden diese empirisch gewonnenen Erkenntnisse neben der bereits angeführten Privacy-Calculus-Theorie auch durch die Technological-Frames-Theorie von Orlikowski und Gash (1994).

Quantitative Studie – Entwicklung und Evaluation eines Ursache-Wirkungs-Modells

Entsprechend dieser Erkenntnisse und im Hinblick auf das Leitthema der Arbeit: *Preisgabeverhalten sensitiver Informationen von Mitarbeitern in Unternehmenssoftware* wurde ein Kosten-Nutzen-Modell[3] entwickelt. Um die Validität dieses Forschungsmodells und den darin enthaltenen neuen Konstrukten zu prüfen, erfolgte eine quantitative Untersuchung, die mittels einer Kovarianzbasierten Kausalanalyse ausgewertet wurde. Das entwickelte Forschungsmodell wurde mittels einer Umfrage in einem weltweit agierenden Großunternehmen mit Sitz in Europa evaluiert (Teilnehmerzahl: 327).

Das Modell zeigt auf, dass Mitarbeiter ihre Entscheidung, sensitive Informationen preiszugeben oder einem System mit Widerstand zu begegnen auf einer Kosten-Nutzen-Kalkulation basieren. Im Konkreten verfährt das Modell wie folgt.

[3] Kosten-Nutzen-Modell: basierend auf dem „Privacy-Calculus"-Ansatz von Dinev und Hart (2006)

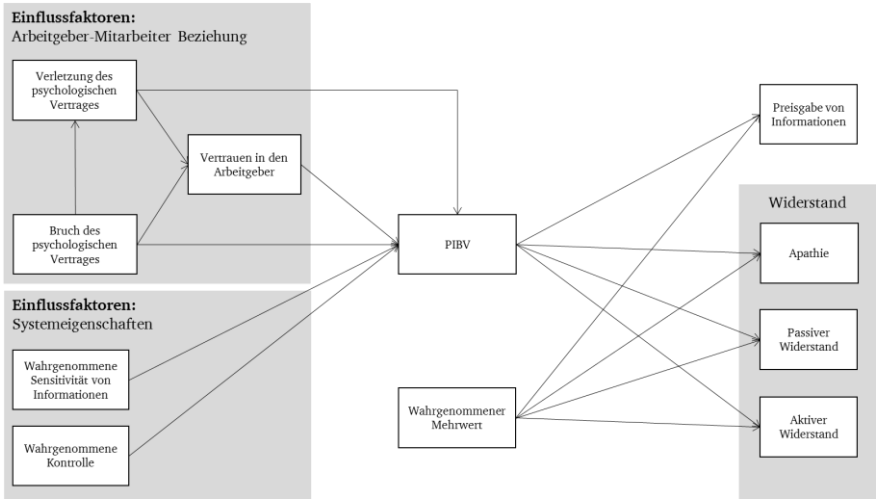


Abbildung 1: Kosten-Nutzen-Modell

Die Datenanalyse ergab grundlegende Abhängigkeiten zwischen spezifischen Systemeigenschaften, Einflussfaktoren bezüglich der Arbeitgeber-Mitarbeiter-Beziehung, PIBV, wahrgenommener Mehrwert und unterschiedlichem Reaktionsverhalten von Mitarbeitern (vergleiche Abbildung 1). Insbesondere hat sich herausgestellt, dass PIBV einen deutlich negativen Einfluss auf das Preisgabeverhalten und dementsprechend positiven Einfluss auf das Widerstandsverhalten der Mitarbeiter hat. Darüber hinaus kann das PIBV durch den wahrgenommenen Mehrwert für den Mitarbeiter gemindert werden (Kosten-Nutzen-Kalkulation). Systemeigenschaften, sowie das Arbeitgeber-Mitarbeiter-Verhältnis haben einen entscheidenden Einfluss auf das PIBV der Mitarbeiter.

In Summe konnten die quantitativen Ergebnisse die zugrundeliegenden Theorien Privacy-Calculus-Theorie und Technological-Frames-Theorie bestätigen, ferner konnte noch eine weitere Theorie hinzugezogen werden, die das Modell zusätzlich stützt. Hierbei handelt es sich um die Psychologische-Vertrags-Theorie[4] (Robinson und Morrison 2000), deren besonderer Fokus auf der Arbeitgeber-Mitarbeiter-Beziehung liegt.

Praxisstudie – Anwendung des Ursache-Wirkungs-Modells zur erfolgreichen Einführung eines HR-Feedbacksystems

Um zu zeigen, dass das Kosten-Nutzen-Modell in der Praxis anwendbar ist, wurde es abschließend im Rahmen einer Feldphase erprobt. Hierfür wurde eine Praxisstudie durchgeführt, die die Einführung eines HR-Feedbacksystems unter 226 Mitarbeitern an einem

[4] Der psychologische Vertrag beschreibt die subjektive Überzeugung eines Mitarbeiters über die Verpflichtungen und Versprechen, die ein Arbeitgeber dem Mitarbeiter gemacht hat. Diese Überzeugung kann auf Grundlage des Einstellungsgespräches, Erzählungen von Kollegen oder beispielsweise den Medien entstehen und hat nichts mit dem tatsächlichen Arbeitsvertrag zu tun (Robinson und Morrison 2000).

Schweizer Standort eines europäischen Unternehmens begleitete. In Folge der Praxisstudie kam es zu keinem vermeintlichen Implementierungserfolg des genannten HR-Feedbacksystems, da die Annahme des Systems durch die Mitarbeiter gering ausfiel. Durch die wissenschaftliche Begleitmaßnahme in Form des Kosten-Nutzen-Modells konnte jedoch Daten generiert werden, die dem Unternehmen halfen Ursachen für die geringe Teilnahme zu benennen. Im Rahmen eines Workshops, bei welchem die zentralen Erkenntnisse der Praxisstudie nochmals gezielt mit Mitarbeitern behandelt wurden, konnte aufgezeigt werden, dass den Nutzern zum einen der Mehrwert des neuen Systems unklar und zum anderen die Verpflichtung gegenüber der Einführung der gesamten Leitungsebene intransparent war. Somit gelang es abschließend über das erwartete Maß hinaus praxisrelevante Hinweise für zukünftige Implementierungen zu formulieren.

Schlussbemerkung

Im Ganzen zeigt die Arbeit auf, dass die Preisgabe sensitiver Informationen durch den Mitarbeiter in Unternehmenssoftware durch unterschiedliche Faktoren beeinflusst wird. Berücksichtigt man die Erkenntnisse dieser Arbeit können entsprechende Unternehmenssoftwaresysteme sowohl erfolgreicher eingeführt werden als auch ihr tatsächliches Potential entfalten.

Table of Contents

List of Abbreviations

ACM	Association for Computing Machinery
ANOVA	Analysis of Variance
AP	Apathy
AR	Active Resistance
AVE	Average Variance Extracted
B	Benefits
B2C	Business to Customer
BISE	Business & Information Systems Engineering
CI	Confidence Interval
CFI	Comparative Fit Index
CHB	Computers in Human Behavior
CLF	Common Latent Factor
CMB	Common Method Bias
CR	Construct Reliability
D	Draft
DF	Degree of Freedom
DSS	Decision Support Systems
e.g.	For example (Exempli Gratia)
EJIS	European Journal of Information Systems
EIS	Enterprise Information Systems
ESS	Enterprise Social Systems
et al.	And others (Et Aliae)
FLC	Fornell-Larcker Criterion
H	Hypothesis
HR	Human Resources
ICIS	International Conference on Information Systems
ID	Intention to Disclose
i.e.	That is (Id Est)
IR	Indicator Reliability
IS	Information System
ISF	Information Systems Frontiers
ISR	Information Systems Research
IT	Information Technology
IUIPC	Internet User's Information Privacy Concern
JCMC	Journal of Computer-Mediated Communication
JCP	Journal of Consumer Psychology
JIM	Journal of Interactive Marketing
JIT	Journal of Information Technology
JSIS	Journal of Strategic Information Systems
KPI	Key Performance Indicator

ME	Mediator
MISQ	Management Information Systems Quarterly
MO	Moderator
n	Sample Size
n.a.	Not Available
NNFI	Non-Normed Fit Index
n.s.	Not Significant
OSN	Online Social Network
p.	Page
PC	Perceived Control
PCB	Psychological Contract Breach
PCT	Privacy Calculus Theory
PCV	Psychological Contract Violation
PI	People Involvement
PIBV	Perceived Information-Based Vulnerability
PIS	Perceived Information Sensitivity
PLS	Partial Least Square
PR	Passive Resistance
P3P	Platform for Privacy Preferences Project
R&D	Research and Development
REIS	Revealing Enterprise Information System
RMSEA	Root Mean Squared Error of Approximation
SET	Social Exchange Theory
SID	Sensitive Information Disclosure
SIGMIS	Special Interest Group of Management and Information Systems
SNS	Social Network System
SRMR	Standardized Root Mean Square Residual
T	Trust into Employer
TAM	Technology Acceptance Model
TLI	Tucker-Lewis Index
VHB	Verband der Hochschullehrer für Betriebswirtschaft e.V.
vs.	versus
U.S.	United States
UTAUT	Unified Theory of Acceptance and Use of Technology

List of Figures

List of Tables

1. Introduction

1.1. Motivation and Problem Definition

Enterprise software solutions that need sensitive information disclosure from employees, to be successful, are becoming more and more important for companies. Organizations realize the power of social software to increase communication among employees, to improve knowledge exchange, and to expand the interaction between the employee and the employer (Bughin, Chui, and Miller 2009; Caya and Nielsen 2009; Kügler, Dittes, et al. 2015). For instance, the McKinsey Global Institute forecasts that 70% of all companies will have implemented social software by the end of 2017 (Bughin 2015). Furthermore, the HR analytics trend enables companies to gather and analyze employee data in as little as a minute (Fecheyr-Lippens, Schaninger, and Tanner 2015). When looking outside the company, user-generated content and activities are proven to be a highly valuable source for spreading, filtering and allocating information (Kwak et al. 2010). From the company perspective this indicates that such solutions offer the possibility to collect and to analyze employee-generated content and their work behavior (Chui et al. 2012; Kügler and Smolnik 2013; Leonardi, Huysman, and Steinfield 2013). Nevertheless, employees might perceive a threat and intrusion into their private lives. In order to benefit from the whole potential of solutions that need employees to disclose sensitive information, it is vital to take the employee's perspective into account and to consider its importance when implementing such systems and furthermore, using the collected information for analysis and future decisions.

Besides social software solutions, several other applications – such as employee engagement tools (e.g., TemboStatus), health and well-being platforms (e.g., wellhub, Alyfe), and workforce collaboration solutions (e.g., slack, SAP Jam) – are valuable sources of employee-generated content. Traditional solutions, such as employee surveys, are increasingly perceived as outdated, and employee-mood-measurement providers tackle the market with new solutions, demanding information from employees for data analytics and insights. The purpose of these enterprise information systems is to pinpoint employee concerns, foster collaboration, observe long-term trends, monitor the impact of company programs, provide input for future decisions, address new communication channels, conduct organizational behavior research, assist in change management, and provide symbolic communication with stakeholders. In spite of the potentials of such solutions, emerging studies show that not all employees consuming these applications realize the solution's benefits from information provision (DiMicco et al. 2008; Jackson, Yates, and Orlikowski 2007).

Analogous to social networking software in the leisure space, the success of such solutions is user-driven. For example, in contrast to the usage of conventional software in the office, *Employee Blogs*, imply the social interaction and self-disclosure of employees. As a result, implementing such solutions in the workplace refers to dimensions that go beyond the known Technology Acceptance Models, as employee dislcosure of sensitive information is vital for the success of such solutions. Nevertheless, the employee's intentions to disclose sensitive information and related influencing factors have received little scientific attention. While a few

studies exist that provide promising first insights, their majority has studied usage success (e.g., Herzog et al. 2013; Larosiliere and Leidner 2012; Wattal, Racherla, and Mandviwalla 2010). This dissertation seeks to fill this void by outlining the academic gap in detail and providing an empirical analysis of factors determining an employee's intention to disclose sensitive information in Enterprise Information Systems (EIS).

1.2. Relevance

1.2.1. Relevance for Practice

The trend of enterprises implementing more and more social software, as well as HR analytics applications, puts the employees' willingness to use these systems into focus. Such systems are becoming crucial in the EIS landscape. Furthermore, HR analytics is gaining ground in organizations and demand that employees disclose sensitive information (Romrée, Fecheyr-Lippens, and Schaninger 2016). For instance, new solutions to monitor employee engagement, well-being and health enable companies to perform real-time analysis and derive conclusions by combining employee information with other organizational records, such as financial or customer data. Companies can expect great additional value from the provided information and, therefore, invest in tools to collect and access HR data (Fecheyr-Lippens et al. 2015). Nevertheless, from an employee's perspective these kinds of EIS are not only perceived as an enrichment, but also as a threat. The availability of sensitive employee information promotes misuse and opportunistic behavior on the employer's side and paves the way to a so called 'transparent human being'. The employees' perception has to be understood and managed by companies. To prevent software implementation failures, companies should know how the employee's sensitive information disclosure (SID) behavior is determined. Even though trends indicate that companies can gain insights from this kind of provided information to make more informed and transparent decisions on their workforce (Momin and Mishra 2015), there are several risks and potential pitfalls that have to be considered when realizing this plan. Companies have to understand that employees might feel threatened by the disclosure of sensitive information in enterprise information systems.

To model this fear the present dissertation introduces a new class of enterprise information systems, called Revealing Enterprise Information Systems (REIS), highlighting the relevant characteristics of such systems which make it much more challenging to introduce them and to achieve the acceptance of employees. Furthermore, the peculiarities that influence the fear of employees that their employer might misuse sensitive information will be emphasized.

1.2.2. Relevance for Theory

From the scientific perspective, there are only insufficiently differentiated insights about usage and sensitive information disclosure behavior in revealing EIS by employees (compare Section 3). Relevant scientific studies about this topic are almost nonexistent (see Section 3.1). The literature about SID does not take the enterprise context into account, even though researchers are demanding this perspective (e.g., Bélanger and Crossler 2011; Richter, Riemer, and vom

Brocke 2011; Smith, Dinev, and Xu 2011). Studies conducted in the area of SID have mainly focused on the Internet context with regard to the people's private lives. Social network systems and e-commerce platforms were considered in particular (e.g., Dinev and Hart 2006; Krasnova et al. 2010; Son and Kim 2008).

Out of the organizational perspective, there are a few studies and scientific contributions surrounding comparable social networks in companies, such as enterprise social networks, enterprise social systems, or Enterprise 2.0 (e.g., Herzog et al. 2013; Kügler and Smolnik 2014; Larosiliere and Leidner 2012; Schoenbachler and Gordon 2002). Those existing studies provide promising first insights, but the majority has focused on measuring the success of social enterprise systems usage and in particular, none has focused on SID. Extant research on the implementation of those systems has mainly focused on their outcomes, such as increased employee performance or support in decision-making (e.g., Herzog et al. 2013; Kügler and Smolnik 2013; Larosiliere and Leidner 2012). Even though research on this topic has received increasing attention in recent years, no exhaustive studies regarding antecedents and outcomes of effective usage and SID have been conducted. It remains unnoticed that these specific EIS cannot exist and be successful without honest user input. It is necessary to understand the reasons and origins of the employee's concerns and drivers to contribute to enterprise information systems, and thereby to understand the success factors for such technologies (e.g., company blogs, enterprise social networks, knowledge sharing systems) within organizations. Consequently, there is a need for research regarding the questions of why and when employees contribute with sensitive information disclosure in enterprise information systems, which are dependent on truthful self-disclosure and employee participation.

Researchers have already become aware that there are contextual differences in the usage of technologies, for example between usage of social media in the organizational context and usage of such technologies in general: *'Our decision to focus on social media use in organizations – as opposed to social media use generally – was informed by research suggesting that peoples' perception of the utility of a technology is formed differently when that technology is used in the workplace rather than outside of it (O'Mahony and Barley 1999; Wellman et al. 1996).'* (Treem and Leonardi 2013, p. 8). This awareness supports the motivation to conduct further research in this area and to make distinctions between the leisure and workplace contexts when using revealing technologies and information systems.

The present dissertation contributes to the systematic investigation of the sensitive information disclosure behavior of employees in enterprise information systems and further delivers knowledge gain in the research area of privacy. For this purpose, on the one hand, qualitative and quantitative research about influencing factors will be conducted. On the other hand, existing theories of SID research will be extended with the goal to take the organizational context and peculiarities into account. Thereby the employer-employee relationship will be considered in particular.

1.3. Goals of the Work

The purpose of this work is the sophisticated investigation of essential influencing factors on the employees' sensitive information disclosure (SID) into enterprise information systems. This primary goal is divided into sub-goals, which are presented below.

Within the frame of scientific research and to expand existing research with meaningful new insights, it is necessary that new investigations be embedded into existing literature. Therefore, an analysis of the current scientific research concerning the topic of inquiry and the extended subject area is the first sub-goal of this work. Since the literature on influencing factors on employees' sensitive information disclosure behavior into enterprise information systems is sparse, the relevant literature pool was extended by scientific contributions to sensitive information disclosure in information systems in general. Therefore, the first and the second research questions are:

Research Question 1:
How does existing information systems literature examine sensitive information disclosure?

Research Question 2:
Which factors from existing information systems literature influence the sensitive information disclosure behavior of people?

As the literature review has shown that SID is mainly discussed in privacy literature within the context of social networks, the third research question follows up on this focus. In order to get a more concrete understanding of how general influencing factors of privacy research play a role in the corporate setting, the follow-up question observes the impact of the identified influencing factors from privacy literature on the employee's behavior in disclosing sensitive information in the organizational context. Furthermore, to focus the research perspective into the organizational direction, research question three is answered with regard to the intra-organizational counterpart of social networks – namely enterprise social systems (ESS).

Research Question 3:
How do privacy factors and organizational factors influence employees' beliefs about enterprise social systems and thus, their sensitive information disclosure behavior?

With regard to the primary goal of this work, the question of the concrete influencing factors on the employee's SID and the related possible outcomes have to be concretized and operationalized. Therefore, the operationalization of the findings of research questions one to three are reflected in research question four and five. Building upon the previous research questions, the aim of these sub-goals is to observe the influencing factors and outcomes which play a significant role when examining the perceived vulnerability of employees through sensitive information disclosure. In contrast to the previous research question, which focused on the release of information into ESS, in particular, the follow-up research questions will focus on a broader range of enterprise information systems where employees have to reveal sensitive information and, therefore, perceive a potential vulnerability based on their provided information. Consequently, the related section will introduce a new class of EIS, called Revealing Enterprise Information Systems (REIS) and new constructs, called perceived information-based vulnerability (PIBV) and resistance against REIS usage. The developed

research model and related research questions are tested by a quantitative study in a globally acting company with headquarters in Europe.

Research Question 4:
How is the perceived information-based vulnerability of employees influenced by the employer-employee relationship and specific characteristics of revealing enterprise information systems?

Research Question 5:
How are perceived information-based vulnerability of employees and the perceived benefits from disclosure affecting the employees' usage of revealing enterprise information systems?

In addition to that, a practical case study was conducted to further understand the PIBV of employees and the usage behavior of revealing enterprise information systems. The case study accompanied the implementation of a REIS among 226 employees in a Swiss location of a European company. The goal was to gather insights on the practical applicability of the developed PIBV model. The results were used to derive measures for increasing the employees' intention to disclose in REIS.

1.4. Structure of the Work and Study Organization

The structure of the work is based on the described research goals and several stages of how the research is organized (see Figure 1).

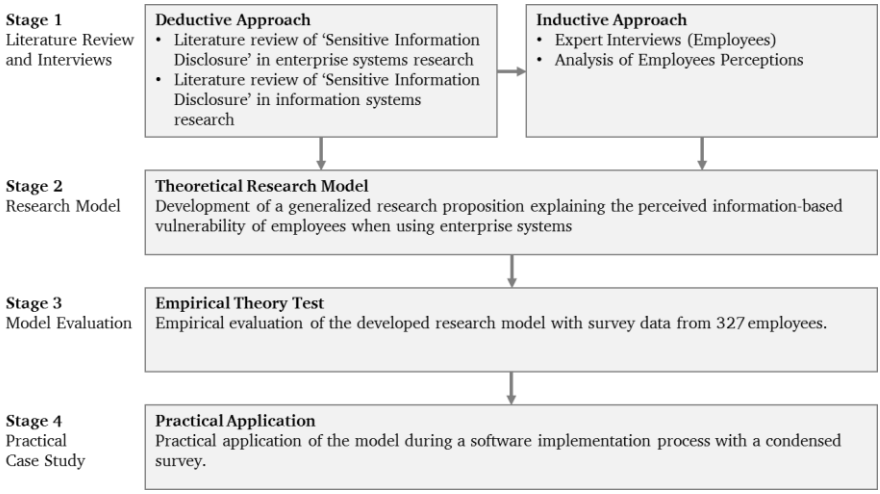


Figure 1: Research Organization

After the introduction section (Section 1) and the definition of basic terms in Section 2, the first stage was entered (according to Figure 1). In this phase, the focus was to better understand the problem space of this work. Therefore, a deductive and inductive approach was chosen to analyze the challenges of the employee's SID in enterprise information systems. Following this procedure, in Section 3 a review and an analysis of the existing information systems literature on SID is given. The first and second research questions will be answered in this section. As a

second step, to better understand the problem space, semi-structured expert interviews were conducted and analyzed in Section 4. After describing the scientific approach for gathering qualitative data, an exploratory study was conducted with 21 experts, in order to answer the third research question. Based on the analysis of the problem space a generalizable research model was developed in stage two (according to Figure 1). The model explains why and when employees might fear vulnerability from sensitive information disclosure in enterprise information systems (Section 5). After describing the conceptual foundations, concrete research hypotheses were derived. The hypotheses were analyzed and tested with data from a survey (n=327). Employees were asked to evaluate their perception of an exemplary REIS (stage 3 in Figure 1). To answer research questions four and five, a statistical analysis of the related causal model was conducted and discussed. Furthermore, Section 6 includes a practical case study (stage 4 in Figure 1). The introduction of a REIS was accompanied with a practical study based on the causal model and survey of part 5 to test for the potential PIBV of the software solution. Section 7 summarizes the results of the work, and the essential implications for research and practice are discussed.

2. Basic Definitions

In the following section, the necessary basics for the understanding and separation of this research are explained. Accordingly, definitions and explanations of the central terms and concepts of the work will be illustrated below.

2.1. Sensitive Information

Against the background of the research goal, namely the examination of the employee's sensitive information disclosure in EIS, the term sensitive information and directly related constructs – *private information* and *personal information* - are going to be clarified in this subsection.

Dinev et al. (2013) define the sensitivity of information as *'a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent.'* (p. 302). Even though the authors define the information type as *'specific personal information',* literature on this topic also talks about *private information* as sensitive information items (e.g., Bélanger, Hiller, and Smith 2002; Liao, Liu, and Chen 2011). Private information are information types that cannot be used to identify someone, like gender, drinking or drug habits, sexual preferences and orientation, or opinions (e.g., Gross and Acquisti 2005; Krasnova et al. 2010). Whereas personal information is all information that can be used to identify someone, such as a social security number, street address or e-mail (Liao et al. 2011). Both types of information can evoke a feeling of discomfort when someone demands disclosure (Liao et al. 2011). This might, of course, depend on the context and on the external agent, asking for the information. For instance, when an employer requests the disclosure of a social security number, someone might not hesitate to provide it, since the external agent is represented by his company. However, if an e-commerce website would ask for the same personal information, the same individual might decide not to offer that information because of the unknown goal the agent is pursuing. The same might hold true for private information. When an employer is asking for information about the employee's health, it might be perceived as more sensitive than when a friend is asking for the health status. The more information is seen as sensitive, be it private or personal information, the more risky people perceive the release of this information to be (Li, Sarathy, and Xu 2011). It can be concluded that private as well as personal information can be sensitive information. It is dependent upon the usage context and the perception of the person who owns the information. Considering the goal of this research that the feeling of employees when disclosing sensitive information into EIS should be in focus, there will be no distinction between personal or private information types. In this research, sensitive information is referring to both personal and private employee information.

2.2. Sensitive Information Disclosure

Sensitive Information Disclosure in General

Collins and Miller (1994) describe self-disclosure of information as any message about oneself that a person communicates to another person. SID refers to the extent to which individuals

intentionally and voluntarily expose their selves to others, including opinions, feelings, thoughts and experiences (Derlega et al. 1993). Following Altman and Taylor (1973) SID has three dimensions: depth, breadth, and duration. Whereas depth is referring to the intimacy of information, breadth is describing the amount of information areas which are disclosed (e.g., family, age, work, sexual orientation), and duration is the time spent on revealing. As sensitive information disclosure is a sign of intimacy and trust, it was shown by Collins and Miller (1994) that people tend to disclose more to people they like. Furthermore, they identified that individuals like people more when they disclose sensitive information to them.

Although the goal of this research is to analyze the employee's SID behavior in enterprise information systems, it is important to understand that SID, in general, supports relationship building and maintenance and has to be treated carefully. Moon (2000) suggests that people consider information systems as 'social actors' when interacting with them. Even though people are aware that IS do not react with intentions and feelings like humans, they tend to answer to IS in similar ways (Moon 2003).

Sensitive Information Disclosure in Information Systems

As already described, SID includes the voluntary and intentional sharing of personal or private information with others. In IS literature *others* is mostly represented not through a physical person, but rather through an online vendor, a social network provider or other social network users (e.g., Krasnova et al. 2012; Metzger 2004; Posey et al. 2010). SID on social network sites takes place when a community member shares details, moods, news, opinions, ideas or beliefs on the social network web page or by communicating with other members (Krasnova et al. 2012). When considering SID in the context of e-commerce, disclosure is required when someone wants to make transactions over the Internet (Dinev and Hart 2006). This can include credit card information or identifiers, as well as any other kind of information that is needed for purchasing goods or services through the Internet or to register at websites (Dinev and Hart 2006). Disclosed information can be used to form conclusions about a user's habits, personality, performance, and tendencies (Kluemper and Rosen 2009). Overall, SID in IS is essential for the business models of many Internet platforms, as it supports user involvement, facilitates individualized advertisement, or enables Internet transactions.

When mapping SID in IS to the organizational context, SID of employees would be an *employee's voluntary and intentional exposure about oneself to their employer through enterprise information systems* (based on Posey et al. 2010). In the present context, SID in EIS would comprise the disclosure of all kinds of information that would make employees feel that conclusions could be made about their working habits, personality, performance at work or even their private life.

3. Sensitive Information Disclosure in Information Systems – A Literature Review

In order to answer the first (How does existing information systems literature examine sensitive information disclosure?) and second research question (Which factors from existing information systems literature influence the sensitive information disclosure behavior of people?), the following section aims at providing a summary of the literature on an employee's SID behavior. Therefore, this subsection will first provide an overview of the relevant literature related to influencing factors of EIS users' SID behavior. Afterwards, an expanded review of the literature on the SID behavior of IS users in general will be done. Furthermore, it will be illustrated how SID is examined in past research and which underlying theories are used for investigation. Based on the existing literature, influencing factors are going to be identified, and their mode of action will be explained in detail. According to that, research gaps are presented and recommendations for future research derived.

To identify existing relevant literature, the databases Google Scholar, Business Source Premier, PsycARTICLES, and PsycINFO were screened for relevant search terms in the title and abstract of included journals. As recommended by vom Brocke et al. (2009), proceedings of the well-known conference *International Conference on Information Systems* (ICIS) have been included in the search process.

3.1. Sensitive Information Disclosure in Enterprise Information Systems

As a first step for the review of the relevant literature, a search string was developed. As the focus of the study was on literature about the readiness of employees to disclose sensitive information into enterprise information systems, several crucial elements had to be mirrored in this string. First, the relevant target group of users – namely, the employee – had to be included in the search to make sure that only literature that was dealing with the employee and the organizational environment was included in the review. Additionally, it was important that the contributions were about the employee's personal, private or sensitive information sharing behavior within enterprise information systems. Therefore, those aspects had to be considered as well. The following expression shows the resulting keyword string for the search of relevant literature:

*('Employee' OR 'Workforce' OR 'Staff') AND ('Sensitive' OR 'Personal' OR 'Private' OR 'Self-Disclosure') AND ('Information' OR 'Data') AND ('*Information System' OR 'Social' OR 'Enterprise System')*

In a second step, the resulting articles were screened to identify those contributions which included statements regarding interdependencies between influencing factors and an employee's SID behavior or willingness to self-disclose in EIS. Afterwards, a backward and forward search was conducted by analyzing the resulting literature pool about relevant reference and referencing research. The search resulted in 60 articles and conference proceedings. In the end, the pool of contributions was screened to extract the relevant papers dealing with influencing factors. After the extraction, only two relevant contributions remained which addressed the topic

in focus – Buettner (2015) and Schoendienst et al. (2011). Since there were only two content-related relevant contributions the quality of the journals was neglected. Nevertheless, it should be considered that the publication of Buettner (2015) was published on a C ranked conference (the Hawaii International Conference on System Sciences) in the VHB-JOURQUAL 3 ranking, which indicates lower quality of the proceeding.

The literature search showed that there are very few to no relevant studies examining the topic in focus. The two identified contributions deal with the usage of social network systems (SNS) within the company. Schoendienst et al. (2011) examined an employee's intention to actively contribute to micro-blogs in an enterprise and related influencing factors. They define the intention to contribute/disclose as the posting of messages with the goal to share information, contribute to other content and respond to other users of the blog. They concluded that this kind of information sharing might be sensitive for an employee since provided information was directly linked to the user. Therefore, supervisors could, for example, track postings to monitor the employee. Furthermore, they noted that employees could perceive the demanded information or provided content as sensitive because it was partially dealing with topics about private life and personal information, and hence could have an adverse impact on their privacy. They concluded that concerns about privacy have a negative impact on the intention to contribute to blogs with perceived sensitive information. Nevertheless, they not only identified inhibitors but drivers as well, such as the employee's expectancy on job performance gains. Moreover, Buettner (2015) investigated the employee's resistance behavior concerning the willingness to disclose information of company internal social networks. Like that of Schoendienst et al. (2011), Buettner's research revealed that privacy concerns have an adverse impact on the intention to use an internal SNS. Additionally, he found that perceived ease of use and the perceived usefulness of a system increase the usage intention of employees.

In conclusion, the employee's SID in EIS has not been studied in detail yet. The two identified significant contributions have elaborated on the impact of privacy concerns, as well as the perceived benefit of job performance gains on the usage of company internal social networks in particular. The chosen context of social networks might be intuitive since this kind of EIS demands that users reveal sensitive information about themselves.

As several researchers (e.g., Richter et al. 2011; Treem and Leonardi 2013) have already stated that research on the willingness of employees to contribute to organizational SNSs with sensitive information is missing, the finding of this subsection is not unexpected. As both papers also accentuate that there is missing research on SID in the organizational context and furthermore mainly base their research on literature focusing on public SID or technology acceptance, the present study follows this approach and will provide an exhaustive literature review on public SID as the first step towards SID in EIS. Thus, to get a better understanding of the construct *sensitive information disclosure,* the research will be extended by taking a deeper look into the IS literature on SID in general in the following subsection.

3.2. Sensitive Information Disclosure in Information Systems

Since the resulting relevant literature pool about an employee's SID behavior is sparse, and in order to better understand the construct SID in IS, this subsection gives a broader overview of the research on a user's SID in software. The overarching goal is to obtain more insights about the influencing factors on people's SID behavior and in turn get a foundation for further research on the employee's SID in EIS. Therefore, this subsection will outline how SID was examined in the past. After the description of the method of analysis, there will be a brief overview of the relevant literature. Subsequently, to better understand the structure and composition of SID and the related influencing factors, an analysis of the applied theories and frameworks in past research is conducted. The construct SID itself will be studied from several perspectives, including the applied context, the design of the construct and the dimensionality and specification of *'sensitive information'*. In the end, in order to gain a full view of the application of the construct in literature, the influencing factors, as well as the mediating and moderating variables, will be examined.

The literature search process was identical to the one of the previous overview of research on the employee's SID behavior (subsection 3.1). Relevant databases were screened with the following search term, related to an information system user's SID behavior:

((‘Self-Disclosure’ OR ‘Disclos’) AND (‘Behavior’ OR ‘Intentions’) AND (‘Online’ OR ‘Internet’)) OR ((‘Willingness’ OR ‘Intention*’) AND (‘Disclose’ OR ‘Share’ OR ‘Reveal’ OR ‘Expose’ OR ‘Provide’) OR (‘Personal’ OR ‘Private’ OR ‘Sensitive’) AND (‘Information*’ OR ‘Data*’) AND (‘Online’ OR ‘Internet’))*

Relevant articles and contributions were analyzed to identify those contributions which included statements regarding the SID behavior of information system users. Afterwards, a backward and forward search was conducted by analyzing the resulting literature pool's relevant reference and referencing research. The resulting literature pool of 164 articles and conference proceedings was screened to identify relevant literature regarding interdependencies between influencing factors on the SID behavior of software system users. This filtering resulted in a reduced literature fund of 56 scientific contributions. In the last step, the quality of the literature had to be ensured. Therefore, the proceedings and articles that did not have a high impact, or were not published in a high-quality journal or conference, were excluded from the selection. The VHB (Verband der Hochschullehrer für Betriebswirtschaft e.V.) Ranking was used as a criterion to identify high-quality journals in the cross-disciplinary literature search. Additionally, two relevant articles were included from the Journal of Computer-Mediated Communication (JCMC) out of the marketing discipline and from Computers in Human Behavior (CHB). The resulting list of relevant journals and conference proceedings are shown in Table 1.

Discipline	VHB Rank	Resulting Journals and Conferences	Abbreviation
Information Systems	A+	MIS Quarterly	MISQ
	A+	Information Systems Research	ISR
	A	European Journal of Information Systems	EJIS
	A	International Conference on Information Systems	ICIS
	A	Journal of Information Technology	JIT
	A	Journal of Strategic Information Systems	JSIS
	B	ACM SIGMIS	SIGMIS
	B	Business & Information Systems Engineering	BISE
	B	Decision Support Systems	DSS
	B	Information Systems Frontiers	ISF
Marketing	B	Journal of Interactive Marketing	JIM
	B	Journal of Consumer Psychology	JCP
	-	Journal of Computer-Mediated Communication	JCMC
Others	-	Computers in Human Behavior	CHB

Table 1: Relevant Literature Sources

All identified significant sources were analyzed. Consequently, a brief overview of the research context, the dependent and independent variables, and the moderators/mediators investigated is given in the following table (Table 2). Regarding the content of the study results, the commonality is that the impact of information system characteristics, benefits and/or threats regarding information disclosure are in the focus of the related research models. Compared to the structured literature search on SID in EIS, the literature search shows that several studies deal with the development of influencing factors on SID concerning the general IS context.

Source and Research Context	Influencing Factors and Interdependencies [a]	Moderators/Mediators [a]	Dependent Variable [a]
Anderson and Agarwal 2011, ISR Health Information	Electronic Health Information Privacy Concern (-)	Intended Purpose (Mo; +)	Willingness to Provide Access to Personal Health Information
		Requesting Stakeholder (Mo; +)	
		Type of Information (Mo; n.s.)	
	Trust in Electronic Medium (+)	Intended Purpose (Mo; n.s.)	
		Requesting Stakeholder (Mo; n.s.)	
		Type of Information (Mo; n.s.)	
	Health Status Emotion (-)		
Bansal et al. 2010, DSS Health Information	Health Information Privacy Concern (-)		Intention to Disclose
	Trust in the Health Website (+)		
	Prior Positive Experience with Website (+)		
Chen and Sharma 2013, ISF SNS	Trust (+)		Self-Disclosure
	Identification (+)		
	Reciprocity (+)		
Dinev and Hart 2006, ISR E-Commerce	Internet Privacy Concerns (-)		Willingness to Provide Personal Information to Transact on the Internet
	Perceived Internet Privacy Risk (-)		
	Internet Trust (+)		
	Personal Internet Interest (+)		

Source and Research Context	Influencing Factors and Interdependencies [a]	Moderators/Mediators [a]	Dependent Variable [a]
Dinev et al. 2008, JSIS Internet	Perceived Need for Government Surveillance (+)		Willingness to provide personal information required to complete transactions on the Internet
	Privacy Concerns Related to Information Finding (-)		
	Privacy Concerns Related to Information Abuse (-)		
	Government Intrusion Concerns (n.s.)		
Gerlach et al. 2015, JSIS, SNS	Privacy Policy Permissiveness (-/-)	Perceived Privacy Risk (Me, -)	Willingness to Disclose
Hollenbaugh and Ferris 2014, CHB SNS	Extraversion (+)		Self-Disclosure (Depth)
	Motive: Virtual Community (+)		
	Openness, Self-Esteem, Conscientiousness, Neuroticism, Agreeableness, Sex, Age; Social Cohesion; Motives: Companionship, Exhibitionism, Relationship Maintenance, Passing Time (n.s.)		
	Self-Esteem (-)		Self-Disclosure (Breadth)
	Openness (+)		
	Neuroticism (-)		
	Motive: Relationship Maintenance (+)		
	Extraversion, Conscientiousness, Agreeableness, Sex, Age; Social Cohesion; Motives: Virtual Community, Companionship, Exhibitionism, Passing Time (n.s.)		
	Motive: Exhibitionism (+)		Self-Disclosure (Amount)
	Motive: Relationship Maintenance (+)		
	Extraversion, Openness, Self-Esteem, Conscientiousness, Neuroticism, Agreeableness, Sex, Age; Social Cohesion; Motives: Virtual Community, Companionship, Exhibitionism, Passing Time (n.s.)		

Source and Research Context	Influencing Factors and Interdependencies [a]	Moderators/Mediators [a]	Dependent Variables [a]
Hui, Teo, and Lee 2007, MISQ E-Commerce	Monetary Incentive (+)		Consumer Disclosure
	Amount of Information Request (-)		
	Privacy Statement (+)		
	Positive Internet shopping experience (+)		
	Privacy Seal (n.s.)		
Krasnova et al. 2010, JIT SNS	Perceived Privacy Risk (-)		Self-Disclosure
	Convenience in Relationship Maintenance (+)		
	Relationship Building (+)		
	Enjoyment (+)		
	Self-Presentation (n.s.)		
Krasnova et al. 2012, BISE SNS	Enjoyment (n.s.)	Individualism (Mo)	Self-Disclosure
	Privacy Concerns (-)	Uncertainty Avoidance (Mo)	
	Trust in SNS Provider (+)	Individualism (Mo)	
	Trust in SNS Members (+)	Individualism (Mo)	
	Gender (n.s.)		
Li and Sarathy 2007, ICIS E-Commerce	Privacy Risk Beliefs (-)		Behavioral Intention to Disclose Information
	Privacy Protection Beliefs (+)		
	Perceived Usefulness (+)		
	Monetary Rewards (-)	Perceived Relevance (Mo; +)	
Li et al. 2011, DSS E-Commerce	Privacy Risk Belief (-)		Behavioral Intention to Disclose Information
	Privacy Protection Belief (+)		
	General Privacy Concern (-)		

Source and Research	Influencing Factors and Interdependencies [a]	Moderators/Mediators [a]	Dependent Variables
Malhotra et al. 2004, ISR Internet	Risk Beliefs (-)		Behavioral Intention towards Releasing Personal Information
	Internet Users' Information Privacy Concern (n.s./+/-)	Trusting Beliefs (Me)	
	Trusting Beliefs (+)	Risk Beliefs (Me)	
	More Sensitive Information (-)		
McKnight et al. 2002, ISR E-Commerce	Trusting Beliefs (+)		Give Information
	Disposition to Trust (n. s.)		
	Institution-Based Trust (n. s.)		
Metzger 2004, JCMC E-Commerce	Trust in a Company's Web Site (+)		Depth of Online Information Disclosure
	Past Online Disclosure (+)		
	Trust in a Company's Web Site (+)		Breadth of Online Information Disclosure
	Past Online Disclosure (+)		
Posey et al. 2010, EJIS Online Community	Social Influence to Use Online Communities (+)		Self-Disclosure
	Social Benefits (Perceived Reciprocity) (+)		
	Perceived Anonymity (n.s.)		
	Privacy Risk Beliefs (-)		
	Perceived Online Community Trust (+)		
	Perceived Individualism (n.s.)		
	Perceived Collectivism (+)		

Source and Research	Influencing Factors and Interdependencies	Moderators/Mediators [a]	Dependent Variables
Son and Kim 2008, MISQ Internet	Information Privacy Concerns (+)		Personal Information Provision Refusal
	Perceived Justice (-)		
	Information Privacy Concerns (+)		Personal Information Misrepresentation
	Perceived Justice (-)		
Schoenbachler and Gordon 2002, JIM Relationship Marketing	Trust in Organization (+)		Willingness to Provide Information
Wakefield 2013, JSIS E-Commerce	Website Trust (+)		Intention to Disclose Personal Information on Unfamiliar Websites
	Website Privacy Beliefs (+)		
	Positive Affect (Enjoy) (+)		
	Negative Affect (-)		
White 2004, JCP E-Commerce	Relational Depth (+/+)	Perceived Disclosure Consequences (Me)	Willingness to Reveal Information Associated with Potential Loss of Privacy (e.g., Address)
	Customized Marketer Benefits Offerings (+)		
	Relational Depth (-/-)	Perceived Disclosure Consequences (Me)	Willingness to Reveal Information Associated with Potential Loss of Face (e.g., Condom use)
	Customized Marketer Benefits Offerings (+)		
Yang and Wang 2009, ACM SIGMIS Internet	Privacy Concern (-)		Information Disclosure Intention
	Information Sensitivity (-)		
	Interaction of Information Sensitivity and Compensation (+)		

Table 2: Literature Overview *Sensitive Information Disclosure*

[a]: (+) = positive effect on the dependent variable; (-) = negative effect on the dependent variable; (n.s.) = no significant effect on the dependent variable; (Me) = mediating effect; (Mo) = moderating effect; In a bracket with two omens, the first omen illustrates the direct effect of the independent variable on the dependent variable and the second omen shows the interdependency of the independent variable on the mediator, of a partial mediating effect

3.2.1. Structural View on Sensitive Information Disclosure

The implementation of *Sensitive Information Disclosure* in literature shows several patterns and differences that influence the conceptualization and measurement of this construct. To understand differences and commonalities among concept and measurement, this subsection provides an exhaustive breakdown of the construct. During the analysis three differences were outstanding – (1) the examined context, (2) the design of SID and (3) the dimensionality and specification of sensitive information. The *examined context* is the environment in which SID and the related model are evaluated and tested (e.g., social network context or e-commerce context). The *design* describes the differences and similarities in how SID is defined, termed and operationalized in literature. The analysis of the *dimensionality* and *specification* describes how literature operationalizes *'sensitive information'* and how different information types are incorporated. Consequently, the construct will be explained and analyzed on the basis of all three characteristics in the following.

Examined Context of Sensitive Information Disclosure

As shown in Figure 2, literature with the focus on SID of software users concentrates on the online context. The primary research context is e-commerce (e.g., Dinev and Hart 2006; Hui et al. 2007; Li and Sarathy 2007; Metzger 2004) and SNS scenarios (e.g., Chen and Sharma 2013; Hollenbaugh and Ferris 2014; Krasnova et al. 2010, Krasnova et al. 2012). Furthermore, research is also found in the electronic health information (Anderson and Agarwal 2011; Bansal et al. 2010) and the general Internet context (Dinev et al. 2008; Malhotra et al. 2004; Yang and Wang 2009). One further study focuses on online relationship marketing (Schoenbachler and Gordon 2002).

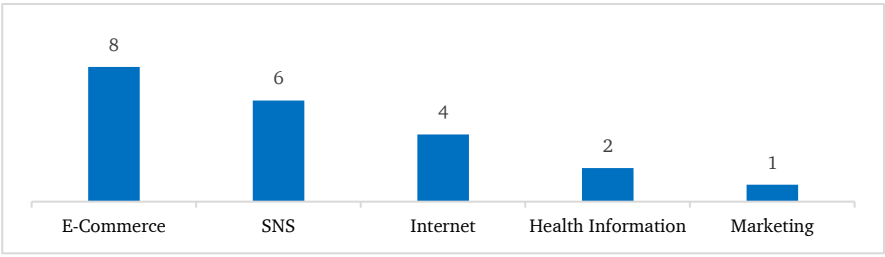


Figure 2: Distribution of Relevant Literature Based on Context

All research areas are centered on information systems that depend on the willingness of users to disclose personal or private information. For instance, a social network system without any personal and private user input or user interaction is useless (Krasnova et al. 2010). The same holds true for online health information platforms where users have to contribute private information about their health status (Anderson and Agarwal 2011). Additionally, on e-commerce websites, potential buyers have to provide personal information to purchase goods and to generate their own benefits from participation and usage (Dinev and Hart 2006). Not

only is the benefit for users dependent upon the sensitive information they offer, but also – and foremostly – the provided information unlocks (additional) value for the platform and software owners through better customer segmentation, data mining possibilities, micro-segmented online advertising or the opportunity for direct communication with their clients (Krasnova et al. 2010). It becomes evident under such considerations that many of these kinds of information systems and their business models are dependent on the willingness of users to provide information to survive.

When considering the research context of this dissertation, this dependence of value on information provisioning might also be valid for the usage of such platforms within a company. For instance, the success of SNS hosted by the employer (Enterprise Social Systems) might be dependent upon similar success factors as external SNS.

Design of the Construct Sensitive Information Disclosure

The design of the investigated dependent variable varies over the relevant literature with regard to *intention to disclose, willingness to disclose* (e.g., Gerlach et al. 2015; Wakefield 2013; Yang and Wang 2009) or *actual SID behavior* (e.g., Chen and Sharma 2013; Hollenbaugh and Ferris 2014; Hui et al. 2007; Krasnova et al. 2010, Krasnova et al. 2012). The *willingness to disclose information* refers to the willingness to reveal the personal information needed to complete Internet transactions (Dinev and Hart 2006). It focuses on the extent of the willingness to insert different sensitive information types, such as credit card information (e.g., Dinev and Hart 2006; Dinev et al. 2008), an address or phone number (e.g., McKnight et al. 2002; Metzger 2004; White 2004), a social security number (e.g., McKnight et al. 2002; Metzger 2004), or information about needs regarding products (Schoenbachler and Gordon 2002). The *intention to disclose information* is defined as *'[…] intentional self-disclosure which refers to the breadth and depth of personal information that one individual willingly provides to another'* (Wakefield 2013, p. 159). Scientific publications assessing the *intention to disclose* are going beyond the *willingness* by additionally measuring the likeliness and probability to disclose sensitive information in IS (Anderson and Agarwal 2011; Bansal et al. 2010; Li and Sarathy 2007; Li et al. 2011; Malhotra et al. 2004; Son and Kim 2008; Wakefield 2013; Yang and Wang 2009). This more detailed approach might lead to a better understanding of the user's purposes and tendencies when using an information system. Moreover, not only intentions are in the focus of such research; the actual *sensitive information disclosure behavior* is an object of investigation as well. Krasnova et al. (2010) describe the real behavior as the extent of information that a person provides on a website. Researchers who analyze the actual behavior mainly focus on the current status of user profiles in social networks and how these profiles represent the true self (Chen and Sharma 2013; Hollenbaugh and Ferris 2014; Krasnova et al. 2010; Posey et al. 2010).

All three construct designs could be identified at the conceptual (naming and definition) and operational (measurement) level. Interestingly, the naming, definition, and operationalization of SID is not consistent regarding the willingness, intention or actual behavior of SID within several publications (see Table 3 – gray highlighted rows). For example, Li and Sarathy (2007)

and Li et al. (2011) name the construct *behavioral SID intention* but define it as *the 'willingness to provide personal information to a specific vendor […]'* (Li et al. 2011, p. 437). Furthermore, when it comes to measurement, they again measure the *behavioral SID intention* with an operationalized scale by Malhotra et al. (2004).

All in all, it can be noted that SID is defined, named, and operationalized in three different ways. However, they are not consistently applied in the relevant contributions. For instance, some researchers define their construct as the *willingness to disclose information* but use the operationalization of the construct *intention to disclose information* (see Table 3). This might lead to inconsistencies and inaccuracies regarding the goal of the specific research and the construct SID, itself.

	Sensitive Information Disclosure		
Literature	Name [a]	Definition [a]	Operationalization [a]
Anderson and Agarwal 2011	W	**X**	I
Bansal et al. 2010	I	I	I
Chen and Sharma 2013	B	B	B
Dinev and Hart 2006	W	W	W
Dinev et al. 2008	W	W	W
Gerlach et al. 2015	W	W	W
Hollenbaugh and Ferris 2014	B	B	B
Hui et al. 2007	B	**X**	B
Krasnova et al. 2010	B	B	B
Krasnova et al. 2012	B	B	B
Li and Sarathy 2007	I	W	I
Li et al. 2011	I	W	I
Malhotra et al. 2004	I	I	I
McKnight et al. 2002	I	I	W
Metzger 2004	B	W	W
Posey et al. 2010	B	B	B
Schoenbachler and Gordon 2002	W	**X**	W
Son and Kim 2008	B	B	I
Wakefield 2013	B	I	I
White 2004	W	**X**	W
Yang and Wang 2009	I	I	I

Table 3: Conceptualization of *Sensitive Information Disclosure*

[a]: B = Actual SID behavior; I = Intention to disclose information; W = Willingness to disclose information; X = Not Defined

Dimensionality & Specification of 'Sensitive Information'

Another recognizable, distinctive feature when taking a more detailed and analytical view on SID is the dimensionality and specification of *'sensitive information'* in the relevant literature. Both aspects have an impact on the measurement of the construct. While *dimensionality* describes the multiplicity of aspects of sensitive information and the detailed operationalization, the *specification* of sensitive information differentiates as to whether information is treated as a generic term or is defined by distinct attributes (see Table 4 for the application methods in the relevant studies).

	Sensitive Information	
Literature	Dimensionality	Specification
Anderson and Agarwal 2011	One	*Distinct*
Bansal et al. 2010	One	Generic
Chen and Sharma 2013	One	Generic
Dinev and Hart 2006	One	*Distinct*
Dinev et al. 2008	One	*Distinct*
Gerlach et al. 2015	One	Generic
Hollenbaugh and Ferris 2014	*Multi*	Generic
Hui et al. 2007	One	*Distinct*
Krasnova et al. 2010	One	Generic
Krasnova et al. 2012	One	Generic
Li and Sarathy 2007	One	Generic
Li et al. 2011	One	Generic
Malhotra et al. 2004	One	*Distinct*
McKnight et al. 2002	One	Generic
Metzger 2004	*Multi*	*Distinct*
Posey et al. 2010	One	Generic
Schoenbachler and Gordon 2002	One	Generic
Son and Kim 2008	*Multi*	Generic
Wakefield 2013	One	Generic
White 2004	One	*Distinct*
Yang and Wang 2009	One	*Distinct*

Table 4: Dimensionality and Specification of *Sensitive Information Disclosure*

When SID is treated as a multi-dimensional construct, the dimensions vary from *depth*, *breadth,* and *amount* of disclosure (Hollenbaugh and Ferris 2014; Metzger 2004; White 2004). Whereas

the *amount* of sensitive information disclosure is defined as the number of disclosures made on a website (Hollenbaugh and Ferris 2014), *depth* is conceptualized by the degree of intimacy and personality of information (Metzger 2004), and *breadth* is characterized by the amount of variety present among topics disclosed on a website (Hollenbaugh and Ferris 2014). By distinguishing between several SID dimensions, researchers can present in greater detail which influencing factors have an impact on which aspects of disclosure, and can ultimately offer more concrete recommendations for practice on how to counteract when people are not disclosing. For instance, the results of this more detailed approach are that different personal variables and different disclosure motives influence the depth, breadth, and amount of people's SID (e.g., Hollenbaugh and Ferris 2014, Metzger 2004, Son and Kim 2008). Even though the multi-dimensional method offers more detailed insights, the most prevalent approach is to examine SID as a one-dimensional construct (see Table 4). Therefore, researchers mainly deal with the provision of *sensitive information* – as a general term – to another party (e.g., Dinev and Hart 2006; Dinev et al. 2008; Hui et al. 2007; Li et al. 2011; Malhotra et al. 2004; Posey et al. 2010).

Furthermore, regarding the specification of the construct it can be determined that publications deal with the construct by measuring it as one of the generic terms – sensitive information, personal information or private information without any precise specification. This means in effect that those researchers chose a universal approach to obtain an understanding of the readiness of software users to disclose sensitive information, independent from any specification of the information item (e.g., Bansal et al. 2010; Gerlach et al. 2015; Krasnova et al. 2010). As already described in Section 2, researchers define sensitive information as either personal information or as private information. For instance, Dinev and Hart (2006) define sensitive information as personal information, which *"[…] refers to the type of information necessary to conduct an online transaction"* (Dinev and Hart 2006, p. 63). It is described as any personal information item that is requested by a system. As another example, Posey et al. (2010) define sensitive information as an individual's voluntary and intentional revelation about their own opinions, emotional states, and experiences in relation to others, which in turn relates to private information rather than personal information. This emphasizes that personal and private information are understood as sensitive information by research on SID.

However, some publications measure sensitive information in a more detailed way by mainly conducting scenario-based studies with multiple information items in order to gain a better understanding of the effects of users' perceived sensitiveness of single information items (see Table 4 – Publications marked with *Distinct*). Information items were, for example, credit card numbers and identifiers, home addresses and other contact information (e.g., Dinev and Hart 2006; Malhotra et al. 2004, Metzger 2004, Yang and Wang 2009), or health information (Anderson and Agarwal 2011). This approach was either used to empirically test causal models with multiple sensitive information specifications, without any further implications regarding those specifications (e.g., Dinev and Hart 2006; Dinev et al. 2008; Hui et al. 2007; Malhotra et al. 2004), or to gather deeper insights about the behavioral differences surrounding the disclosure of different information items, along with related influencing factors (e.g., Anderson

and Agarwal 2011, Metzger 2004, White 2004). Regarding the latter, researchers came to different conclusions about the added value when they examined specific items. For example, Anderson and Agarwal (2011) concluded that it might not make sense to distinguish between objects of the same type (e.g., health information items) but rather to research and compare different types of information (e.g., health information in comparison to financial information). An example of the comparison of different types would be White's (2004) research, where the disclosure behavior of embarrassing information was compared with the disclosure behavior of personal information.

Summary of the Construct Sensitive Information Disclosure

In sum, SID is examined in e-commerce, social network systems, online marketing and the health information context, with the focus on e-commerce and social network systems (see Figure 2). Furthermore, SID is designed in three different ways with regard to the conceptual and measurement level. It is designed as either an intention to disclose information, willingness to disclose information, or the actual information disclosure behavior (see Table 3). Moreover, it is primarily examined as a one-dimensional construct but also investigated with multiple dimensions (see Table 4). In addition to that, researchers specified sensitive information mostly as a generic term. Nevertheless few publications determine sensitive information with multiple distinct information items (see Table 4). Anderson and Agarwal (2011) recommend that this should only be applied when either empirically evaluating a model or when entirely different information items are compared.

3.2.2. Underlying Theories and Frameworks

During the analysis of the relevant literature, it was found that several different underlying theories and frameworks inform the decision of researchers as to which influencing factors on information self-disclosure are applied in their research and how. Therefore, to better understand the structure of the literature this subsection will give an overview of those theories. Furthermore, the dominant theories will be described in detail.

As illustrated in Table 5, the primarily applied theories are the 'Social Exchange Theory' (SET) (e.g., Anderson and Agarwal 2011; Bansal et al. 2010; Chen and Sharma 2013) and the 'Privacy Calculus Theory' (PCT)[5] (Dinev and Hart 2006; Krasnova et al. 2010; Krasnova et al. 2012; Li et al. 2011). The SET emphasizes that people weigh the rewards and costs of a decision whether to participate in social transactions or not (Metzger 2004). When the rewards outweigh the costs, a person is likely to step into the exchange relationship (Krasnova et al. 2010). Whereas SET's primary focus is on relationships and the decision to involve oneself therein, the PCT evaluates the trade-offs that Internet users make between the perceived benefits and costs of SID on websites in particular (Dinev and Hart 2006). Based on the PCT, the willingness to disclose sensitive information is determined via the opposing effects of exchange benefits and contrarily perceived costs (Li and Sarathy 2007). Hence, publications which use the PCT or SET as the

[5] Psychological Contract Theory, itself, is also based on the Social Exchange Theory

underlying framework for their research mainly developed their models as a trade-off model with related influencing factors interacting with the weighing (e.g., Bansal et al. 2010; Dinev and Hart 2006; Krasnova et al. 2010; Wakefield 2013). Costs are either defined as *privacy concern* (e.g., Anderson and Agarwal 2011; Bansal et al. 2010) and/or *privacy risk* (e.g., Krasnova et al. 2010; Li and Sarathy 2007; Posey et al. 2010). Furthermore, benefits are described as the resulting benefits from using an online service, such as *enjoyment* (Krasnova et al. 2010) or *customized marketer benefits* (White 2004). Additionally, researchers also see *trust* as a counterpart to privacy risk or concern (Dinev and Hart 2006; Metzger 2004).

Literature	Underlying Theories
Anderson and Agarwal 2011	Social Exchange Theory; Privacy Calculus Theory
Bansal et al. 2010	Social Exchange Theory; Privacy Calculus Theory
Chen and Sharma 2013	Social Exchange Theory; Social Capital Theory
Dinev and Hart 2006	Privacy Calculus Theory; Expectancy Theory
Dinev et al. 2008	Privacy Calculus Theory
Gerlach et al. 2015	Stimulus-Organism-Response Model
Hollenbaugh and Ferris 2014	Use and Gratification Theory
Hui et al. 2007	Privacy Calculus Theory; Contemporary Choice Theory
Krasnova et al. 2010	Social Exchange Theory; Privacy Calculus Theory
Krasnova et al. 2012	Privacy Calculus Theory; Hofstede
Li and Sarathy 2007	Social Contract Theory; Privacy Calculus Theory
Li et al. 2011	Social Contract Theory; Privacy Calculus Theory; Stimulus-Organism-Response Model
Malhotra et al. 2004	Trust-Risk Framework; Theory of Reasoned Action
McKnight et al. 2002	Cognitive-Trust-Based Literature
Metzger 2004	Social Exchange Theory; Internet-Consumer Trust Model; Electronic Exchange Model
Posey et al. 2010	Social Exchange Theory; Social Penetration Theory; Communication Privacy Management Theory; Hofstede
Schoenbachler and Gordon 2002	Trust
Son and Kim 2008	Theory of Reasoned Action
Wakefield 2013	Social Exchange Theory; Theory of Reasoned Action
White 2004	Social Exchange Theory
Yang and Wang 2009	Social Exchange Theory; Privacy Calculus Theory

Table 5: Applied Underlying Theories on *Sensitive Information Disclosure*

Both PCT and SET were not only applied as single underlying theories for research models, but were also enriched by further theories to gain more detailed and concrete insights on specific

aspects. For instance, Posey et al. (2010) added the 'Social Penetration Theory' and the 'Communication Privacy Management Theory' as further underlying theories to SET. They investigated the desire of individuals for acceptance and relational formation in online communities in the context of their related privacy boundaries within these relationships. Another example stems from Dinev and Hart (2006), who included 'Expectancy Theory' in their research. The examination focused on the fact that people behave in certain ways in order to maximize positive and minimize negative outcomes of the cost/benefit scenario. Their research resulted in a very often cited Privacy Calculus Theory. Most of the research grounding on PCT refers to Dinev and Harts' (2006) Privacy Calculus model as the starting point of their research (Anderson and Agarwal 2011; Bansal et al. 2010; Dinev et al. 2008; Krasnova et al. 2010; Li and Sarathy 2007; Li et al. 2011; Yang and Wang 2009). A further prevalent complementary perspective in research that uses SET and PCT as underlying theory is the trust perspective. Researchers, such as McKnight et al. (2002), Metzger (2004), or Schoenbachler and Gordon (2002) added this point of view, to further understand how trust accompanies cost/benefit weighing and the decision to disclose sensitive information. Chen and Sharma (2013) focused on the impact of social capital on SID of social network users by applying the 'Social Capital Theory'. They examined the effect of reciprocity, identification and trust, which represent vital assets for generating mutual benefits in social relations (Chen and Sharma 2013).

Only a few publications did not focus on SET or PCT and investigated SID from other perspectives. Consequently, Malhotra et al. (2004) concentrated on a *'Trust-Risk Framework'* complemented by the *'Theory of Reasoned Action'* as the foundation for their research model. This approach resulted in a basic model for SID where the interaction of trust and risk beliefs influenced behavioral intention with regard to the release of sensitive information, and in turn affected the actual behavior of people. Additionally, Son and Kim (2008) also focused on the *'Theory of Reasoned Action'* for the investigation of sensitive information provision and the impact of justice on the misrepresentation and refusal of information. An entirely different approach was chosen by Hollenbaugh and Ferris (2014), who examined SID based on the *'Use and Gratification Theory'*, which assumes that individuals' psychological and sociological characteristics, as well as personal motives for using a medium, affect the decision whether to use a medium or not. They adapted the approach and examined how personal motives and characteristics influenced the depth, breadth, and amount of SID.

All in all, the underlying theories indicate that SID is mainly examined from a cost/benefit perspective (PCT and SET), allowing researchers to weigh privacy concerns and risks against perceived benefits of exposure.

3.2.3. Analysis of the Influencing Factors

Internet users are often less than forthcoming and very cautious when it comes to SID on the Internet. As the previous subsection points out, research explains this phenomenon by people's perceived privacy risks (e.g., Krasnova et al. 2010; Li and Sarathy 2007; Li et al. 2011) or privacy concerns (e.g., Dinev et al. 2008; Li et al. 2011; Malhotra et al. 2004) as a cost factor of

disclosure. Furthermore, to compensate these costs scientists found out that there are countermeasures, which increase the willingness of people to disclose sensitive information. They revealed that perceived benefits and trust mitigate perceived privacy risks (e.g., Dinev and Hart 2006). As shown in the relevant literature, trust, privacy concerns, privacy risks, and benefits are the common influencing factors of sensitive information disclosure in IS (e.g., Chen and Sharma 2013; Hollenbaugh and Ferris 2014; Krasnova et al. 2010; Posey et al. 2011). Nevertheless, there are several further factors that influence SID. An exhaustive overview of the influencing constructs on SID with the related literature is given in Table 6.

Construct		Definition	Literature
Benefits	Relationship Maintenance	*'The value users derive from being able to efficiently and easily stay in touch with each other on OSNs.'* (Krasnova et al. 2010, p. 112)	Krasnova et al. 2010; Hollenbaugh and Ferris 2014
	Relationship Building	*'The value users derive from being able to build up new connections to others on OSNs.'* (Krasnova et al. 2010, p. 112)	Krasnova et al. 2010; Hollenbaugh and Ferris 2014
	Reciprocity of SNS Users	*'Reciprocity refers to a shared understanding on continuing relationships of exchange and it involves mutual expectations that a benefit granted now will be repaid in the future.'* (Chen and Sharma 2013, p. 271)	Posey et al. 2010; Chen and Sharma 2013
	Enjoyment	*'The value users derive from having pleasant and enjoyable experiences on OSNs.'* (Krasnova et al. 2010, p. 112)	Krasnova et al. 2010; Wakefield 2013
	Perceived Usefulness	*'[…]attractiveness of the offering is operationalized as perceived usefulness of the products or services.'* (Li and Sarathy 2007, p. 4)	Li and Sarathy 2007
	Customized Marketer Benefits Offerings	*'[…]offerings incorporate consumers' specific preferences […].'* (White 2004, p. 44)	White 2004
	Compensation & Monetary Incentives	*'Compensation […] means not only a reward or monetary incentive but also services and any other form of benefits prized by customers.'* (Yang and Wang 2009, p. 39)	Hui et al. 2007; Li and Sarathy 2007: Yang and Wang 2009

Construct	Definition	Literature

Trust	Trust in the Users of a Website	*'The degree to which an individual believes that those within his or her selected online community are reliable and are trustworthy with information that makes the individual vulnerable.'* (Posey et al. 2010, p. 186)	Chen and Sharma 2013; Krasnova et al. 2012; Posey et al. 2010
	Trust in the Medium	*'Trust beliefs reflecting confidence that personal information submitted to Internet websites will be handled competently, reliably, and safely.'* (Dinev and Hart 2006, p. 64)	Anderson and Agarwal 2011; Dinev and Hart 2006
	Trust in the Online Company/Vendor	*'Trust is the degree to which an organization is perceived to be reliable, competent, benevolent, and to have integrity.'* (Metzger 2004, p. n.a.)	Bansal et al. 2010; Krasnova et al. 2012; Malhotra et al. 2004; McKnight et al. 2002; Metzger 2004; Schoenbachler and Gordon 2002; Wakefield 2013
Privacy Concerns	General Privacy Concern	*'An individual's general tendency to worry about information privacy.'* (Li et al. 2011, p. 437)	Li et al. 2011; Li and Sarathy 2007;
	Internet User's Information Privacy Concern (IUIPC)	*'Information privacy concerns refer to an individual's subjective views of fairness within the context of information privacy.'* (Malhotra et al. 2004, p. 337)	Anderson and Agarwal 2011; Bansal et al. 2010; Malhotra et al. 2004; Wakefield 2013; Yang and Wang 2009
	Privacy Concern	*'Concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular.'* (Dinev and Hart 2006, p. 64)	Bansal et al. 2010; Dinev and Hart 2006; Dinev et al. 2008; Krasnova et al. 2012; Son and Kim 2008;
Privacy Protection Beliefs		*'The subjective probability that consumers believe that a specific online vendor will protect their private information as expected.'* (Li et al. 2011, p. 437)	Li and Sarathy 2007 Li et al. 2011
Privacy Risk Beliefs		*'Risk beliefs refer to the expectation that a high potential for loss is associated with the release of personal information to the firm.'* (Malhotra et al. 2004, p. 341)	Dinev and Hart 2006; Krasnova et al. 2010; Li and Sarathy 2007; Li et al. 2011; Malhotra et al. 2004; Posey et al. 2010;

Construct	Definition	Literature
Privacy Policy Permissiveness	*'The policy's permissiveness is the extent to which the provider is free to pursue data monetization objectives based on its users' data.'* (Gerlach et al. 2015, p. 3)	Gerlach et al. 2015
Privacy Statement	Describes a company's *'policies regarding collected consumer information.'* (Hui et al. 2007, p. 20)	Hui et al. 2007
Information Sensitivity	*'The level of privacy concern an individual feels for a type of data in a specific situation'* (Weible 1993, p. 10). (cited by Yang and Wang 2009, p. 40)	Malhotra et al. 2004 Yang and Wang 2009
Amount of Information Request	*'Number of information items requested.'* (Hui et al. 2007, p. 23)	Hui et al. 2007
Positive Experience	*'Prior positive experience with the […] website.'* (Bansal et al. 2010, p. 143)	Bansal et al. 2010 Hui et al. 2007 Metzger 2004
Relational Depth	*'[…] refer to generally positive, long-term relationships in which relatively high levels of trust and satisfaction have been established […].'* (White 2004, p. 49)	White 2004
Perceived Justice	*'Degree of fairness that an Internet user perceives about online companies' treatment related to information privacy.'* (Son and Kim 2008, p. 508)	Son and Kim 2008
Community Identification	*'Community identification is defined as own conception of self with respect to the defining features of a social group.'* (Chen and Sharma 2013, p. 271)	Chen and Sharma 2013
Social Influence	*'Social influence is the degree to which an individual's beliefs, attitudes and/or behaviors are influenced by others in his or her environment.'* (Posey et al. 2010, p. 184)	Posey et al. 2010
Negative Affect	*'Negative affect is an attitude characterized by nervousness, stress, and fearfulness that a user might experience when contemplating a transaction with an unfamiliar website.'* (Wakefield 2013, p. 163)	Wakefield 2013
Personality Traits	'Big Five' personality traits: John et al.'s (1991) Big Five Inventory (BFI) was used to test extraversion, agreeableness, conscientiousness, neuroticism, and openness.	Hollenbaugh and Ferris 2014

Construct	Definition	Literature
Interest into the Medium	*'Personal interest or cognitive attraction to Internet content overriding privacy concerns.'* (Dinev and Hart 2006, p. 64)	Dinev and Hart 2006
Perceived Need for Government Surveillance	*'Perceived need for the government to have greater access to personal information and to monitor personal activities.'* (Dinev et al. 2008, p. 219)	Dinev et al. 2008
Collectivism	*'Collectivism describes cultures in which people are integrated into strong, cohesive groups that protect individuals in exchange for unquestioning loyalty' (Hofstede 1991; Zhang and Lowry 2008, p. 65).'* (Posey et al. 2010, p. 187)	Posey et al. 2010

Table 6: Influencing Factors on *Sensitive Information Disclosure*

As the previous subsection explained SID and the applied underlying theories, this subsection will give further insights on the examined influencing variables of SID in more detail.

Perceived Benefits

Perceived benefits of disclosure can be found in nearly every research model concerning SID as having a positive impact on the willingness to disclose information (e.g., Krasnova et al. 2010; Posey et al. 2010; White 2004). Depending on the research context – SNS or e-commerce – the construct targets different types of benefits. For instance, in the SNS context benefits are primarily derived from communicating with other people (e.g., building up new relations, maintaining existing relationships, reciprocity of SNS users). Krasnova et al. (2010) revealed that the single value derived from having a good and entertaining experience on a social network is a significant driver of the willingness to self-disclose. Furthermore, Hollenbaugh and Ferris (2014) examined SID as a multi-dimensional construct and revealed that depth of information provision is influenced by the motive of relationship building (in his model called 'virtual community'). Furthermore, the goal to maintain relationships has a positive impact on the amount and breadth of user information provision. Chen and Sharma (2013), as well as Posey et al. (2010), revealed a positive effect of reciprocity of SNS users on the willingness to disclose sensitive information. This means that a user's expectation towards the payback of one's own actions in a social network is critical for interaction and success of SNS.

Literature that analyzes SID on e-commerce sites, defines influencing benefits of SID as either the attractiveness of an offered product or service (Li and Sarathy 2007), monetary reward or compensation (Hui et al. 2007; Li and Sarathy 2007; Yang and Wang 2009), enjoyment and feelings of happiness during the e-commerce experience (Wakefield 2013), or the ability of customers to incorporate their specific preferences on offers through customization (White 2004). Interestingly, research illustrated that monetary rewards are not only a driver of SID, but can also undermine information disclosure when users perceive the asked information as

irrelevant (Li and Sarathy 2007). This finding can be aligned with general findings on consumers and their sensitivity about personal information; since users do not see sensitive information in an economic exchange context (Hoffman, Novak, and Peralta 1999). Nevertheless, other examinations have demonstrated that there are dynamics among information sensitivity and compensation which influence the willingness to disclose information (Hui et al. 2007; Yang and Wang 2009). Yang and Wang (2009) revealed in their experiment that a suitable compensation level, combined with little information sensitivity motivates e-commerce users to disclose more accurate personal information. Depending on the context, monetary rewards and compensation should be treated carefully as a means of exchange for user information. Nevertheless, benefits, in general, have a highly positive impact on the SID of Internet users.

Privacy Concerns, Risk and Protection

As already examined in the previous subsection (Subsection 3.2.1), one research stream in particular has focused on the topic of SID – namely, privacy research. The assumptions seem to be that people tend to avoid SID due to their privacy concerns (e.g., Krasnova et al. 2012; Li et al. 2011; Malhotra et al. 2004), privacy risk beliefs (e.g., Dinev and Hart 2006; Krasnova et al. 2010; Malhotra et al. 2004) and privacy protection beliefs (Li and Sarathy 2007; Li et al. 2011). *Privacy concerns* include the worry about information privacy, the subjective view of fairness regarding privacy, and the concern for the opportunistic behavior of other actors in Internet scenarios. *Privacy risk beliefs* describe the real expectation of user loss associated with SID (Malhotra et al. 2004), and *privacy protection beliefs* are beliefs of a user that online companies are willing to protect the user's disclosed sensitive information (Li et al. 2011).

Regarding **privacy concerns**, the literature distinguishes three types of concern that have an adverse impact on SID – *global privacy concerns* (e.g., Li and Sarathy 2007), an *Internet user's information privacy concern* (e.g., Malhotra et al. 2004) and *privacy concerns as fear for opportunism* (e.g., Dinev and Hart 2006). First, the category of *global privacy concerns* reflect the concern for privacy in general, which includes general beliefs about the Internet as a privacy threat and the overall opinion about concerns regarding privacy issues and invasions (Li and Sarathy 2007; Li et al. 2011; Malhotra et al. 2004). This privacy construct is the most generic one and stems from the offline literature about perceived privacy of people in offline scenarios (see Smith et al. 1996). Second, the *Internet user's information privacy concern* (IUIPC), as developed by Malhotra et al. (2004), reflects a person's perception of fairness or justice in the context of information privacy in IS. This construct is related to the awareness of users about privacy practices, the perceived transparency about the collection of information through online companies and the perceived right to control this collection of information (Anderson and Agarwal 2011; Malhotra et al. 2004; Wakefield 2013; Yang and Wang 2009). When Malhotra et al. (2004) introduced this construct, they revealed that IUIPC only has a weak direct relation to SID, but is mediated by trust and risk beliefs. Nevertheless, subsequent contributions that measured the impact of the construct on SID were able to reveal a direct relation between the two constructs (e.g., Anderson and Agarwal 2011; Wakefield 2013; Yang and Wang 2009). Third, the construct *Internet privacy concerns*, developed by Dinev and Hart (2006), reflects the

concern for the opportunistic behavior of a respondent on the Internet related to information disclosure (Dinev and Hart 2006; Dinev et al. 2008; Son and Kim 2008). The construct refers to the fear of Internet users that submitted information might be misused or used in a way that was not foreseeable by the information provider. Even though three types of privacy concerns can be noted, the boundaries between those constructs are blurry and inexplicit. For instance, Bansal et al. (2010) developed a construct based on Malhotra et al.'s (2004) IUIPC, as well as on Dinev and Hart's (2006a) definition and measurement of privacy concern.

In addition to privacy concerns, the relevant privacy literature also focuses on the **privacy risk beliefs** of users as a primary negative influencing factor on the SID behavior. It refers to a potential loss and to perceived negative consequences related to SID (Dinev and Hart 2006; Krasnova et al. 2010; Li and Sarathy 2007; Li et al. 2011; Malhotra et al. 2004; Posey et al. 2010). The actual construct and measure were developed by Malhotra et al. (2004) to measure the perceived loss and uncertainty of a potential website user when he reveals information. Most of the literature built on this construct and reused or adapted the scale to assess privacy risk beliefs (Krasnova et al. 2010; Li and Sarathy 2007; Li et al. 2011; Posey et al. 2010). It is shown that privacy risk beliefs play a significant role in the disclosure behavior of Internet users in general, as well as SNS users and e-commerce customers in particular.

Furthermore, Li and Sarathy (2007) identified an additional construct related to privacy that influences the decision-making process on whether to disclose information or not – namely, **privacy protection beliefs**. It reflects the beliefs of an individual as to whether an online company is willing to protect the provided information of users as expected (Li et al. 2011). It explains people's confidence that they can protect their information on a website during and after a transaction. Li and Sarathy (2007), as well as Li et al. (2011), stated that protection beliefs and risk beliefs are related, yet distinct facets of information privacy. They identified that *privacy protection beliefs* – if people believe that online vendors protect their information from potential harms – act as a benefit factor of SID and *privacy risk beliefs* as a cost factor for the decision whether to disclose information or not (Li et al. 2011).

In conclusion, it can be said that *privacy concerns*, as well as *privacy risk beliefs* influence a user's SID in a negative way, whereas *privacy protection beliefs* reflect a user's view about the good intention of a company to protect their provided information against harms, and therefore have a positive effect on SID. Interestingly, Li et al. (2011) measured the impact of all three aspects of privacy on SID and revealed that *privacy risk beliefs* (-0.366) have the highest impact on a person's decision whether to disclose sensitive information or not [privacy protection beliefs (+0.189); privacy concerns (-0.153)].

Trust

Trust as an influencing factor on both willingness and actual SID in online environments is mainly understood as a multi-faceted construct founded on the perceived *integrity, reliability, benevolence* and *competence* of online vendors (e.g., Dinev and Hart 2006; Wakefield 2013),

health websites (Anderson and Agarwal 2011; Bansal et al. 2010), and members of social networks or communities (Chen and Sharma 2013; Posey et al. 2010). Online websites use trust as a lever to reduce the perceived risk when visiting a website and increase the propensity to disclose information (Metzger 2004; Posey et al. 2010). In the social network and community context, the focus of trust is on the expectations of a network member that other users in the network will behave predictably, fulfill their commitments, and act fairly (Chen and Sharma 2013). When looking into the context of e-commerce sites and health websites, the primary focus is on trust in the vendor and website provider, and in how they handle submitted information (e.g., Malhotra et al. 2004; Metzger 2004; Wakefield 2013). Furthermore, Dinev and Hart (2006) as well as Anderson and Agarwal (2011) examined trust at the medium level. They analyzed whether trust in Internet websites (as media for information storage or exchange) is a trustworthy environment and how it influences the willingness to provide sensitive information. Both revealed that trust in an Internet website increases SID on that specific site.

As already mentioned, independently of the context of the contributions, four overlapping trust dimensions appear regularly throughout the relevant publications. Based on these dimensions, trust is defined as the degree to which an online vendor or website is perceived to have integrity, to be benevolent, to be competent, and to be reliable (Metzger 2004), whereby *integrity* describes the trustworthiness of a site or vendor, *benevolence* reflects if an Internet site is perceived as fair and non-exploitative, *competence* is the knowledge and professionalism of the web service and page, and *reliability* describes the dependability and ability to carry responsibility (Metzger 2004). Not all dimensions are examined equally. Several publications selected only particular dimensions and applied them to their trust construct (e.g., Chen and Sharma 2013; Krasnova et al. 2012; Posey et al. 2010). In general, trust in a website, a vendor or community facilitates disclosure and at the same time mitigates risk beliefs (Dinev and Hart 2006).

Further Influencing Constructs

In addition to the already stated predominant influencing factors, other constructs such as the sensitivity of requested information (Malhotra et al. 2004; Yang and Wang 2009), the amount of resquested information items (Hui et al. 2007), or prior positive experience with vendors or online communities (Bansal et al. 2010; Metzger 2004) have an impact on the decision process determining whether users disclose information or not. Furthermore, social aspects – such as the influence of other people in the environment or the culture on a user's opinion, attitude, or action (Krasnova et al. 2012; Posey et al. 2010) and the user's identification with the community in a social network (Chen and Sharma 2013) – have an impact on SID in IS. For instance, Krasnova et al. (2012), as well as Posey et al. (2010) examined how cultural dynamics have an impact on the self-disclosure behavior of SNS users. They revealed that collectivism, in general, has a positive impact on SID (Posey et al. 2010). Furthermore, they illustrated that in individualistic cultures, trust in SNS providers and members has a bigger impact on SID than in collectivistic cultures (Krasnova et al. 2012), whereas in uncertainty avoiding cultures privacy concerns have a more adverse effect than in uncertainty tolerant cultures (Krasnova et al. 2012). This means

that people with high individualistic values tend to trust, whereas individuals with lower uncertainty avoiding values have the tendency to ignore privacy concerns (Krasnova et al. 2012). Additionally, Hollenbaugh and Ferris (2014) examined how individual variables such as the 'Big Five Inventory' of John et al. (1991) have an impact on SID in information systems. They found that self-esteem and neuroticism have a negative impact and the personal attribute openness has a positive impact on the breadth of SID. Moreover, the personality trait extraversion increases the depth of self-disclosure in social networks (Hollenbaugh and Ferris 2014).

As examined by Hui et al. (2007) and Gerlach et al. (2015) privacy statements and policies also play a significant role in SNS and e-commerce: Hui et al. 2007 revealed that the existence of privacy statements has a positive impact on the disclosure behavior of the online consumer. Gerlach et al. (2015) dug deeper into the area of privacy statements and found that the permissiveness of privacy policies has a significant impact on SID. They described permissiveness as the extent to which SNS providers are trying to monetize a user's provided data. Furthermore, in the e-commerce context the constructs *relationship depth*, *perceived justice* and *negative affect* influence the decision whether to disclose information on the website or not. White (2004), for example, revealed that a deep connection of a buyer to an online vendor, described as mostly positive and continuous with a rather high level of trust and satisfaction, has a positive impact on SID. Additionally, the perceived justice of an Internet user, reflected in the perceived fairness of an online company's treatment of information privacy, plays a significant role when users decide whether to reveal information or not (Son and Kim 2008). Wakefield (2013) showed that not only enjoyment but also negative affect, characterized by nervousness, fear, or stress experienced by the user when considering a transaction with an unfamiliar online vendor, has an impact on the disclosure behavior of users.

In the context of government surveillance, Dinev et al. (2008) examined the relationship between online government surveillance and the willingness to disclose sensitive information on the Internet. They found that an Internet user's perceived need for government surveillance to have better access to personal information and to monitor activities on the Internet increases SID even though users know that the government collects that information. Moreover, they revealed that the perceived benefit from government surveillance even mitigates privacy concern (Dinev et al. 2008).

In general, relying on the applied theory researchers have found several factors that influence the disclosure behavior of sensitive information. An exhaustive list can be found in Table 6.

3.3. Summary

To the best of my knowledge, there is nearly no relevant literature concerning information disclosure of employees in EIS (except Buettner 2015; Schöndienst et al. 2011). Nevertheless, there is existing research on sensitive information disclosure in several other research areas of IS. For instance, most of the research can be found in the e-commerce and SNS context. Additionally, few publications focused on online marketing and online health information

scenarios. All of these research areas are fields of study where SID plays a significant role in IS success. For instance, as already stated in the definition section of SID (Section 2), SID of social network and e-commerce website users is a decisive factor for a successful business model in this domain. A social network system, such as Facebook, would not be successful if people were not willing to communicate, disclose or share information such as pictures, statuses or interesting articles with others on the network. The same holds true for e-commerce websites. In order to conduct transactions on a website, people have to disclose several sensitive information items, such as credit card information or other personal data.

Furthermore, it can be concluded that SID was designed in research as either behavior, willingness to behave or an intention to act. The *willingness* to disclose sensitive information was mainly related to the readiness of users to publish distinct information items and to find out which of these items were perceived as more delicate and worth protecting (e.g., Dinev and Hart 2006). The *intention* to disclose sensitive information was understood and measured as the likeliness, willingness, and probability of an individual to provide sensitive information (e.g., Bansal et al. 2010) and hence included the willingness to disclose information. When it comes to the intention of people, it is shown that behavioral intentions can solidly predict the actual behavior of individuals (Ajzen 1991; Webb and Sheeran 2006). Therefore, behavioral intentions were often applied as a substitute for the real behavior of people in privacy studies (e.g., Malhotra et al. 2004; Son and Kim 2008; Wakefield 2013; Yang and Wang 2009). Nevertheless, research that focused on the actual information disclosure behavior conceptualized it as the actual act of providing information or the extent to which a user has revealed information on a website (Krasnova et al. 2010). When taking a deeper look at the conceptualization and operationalization of the construct SID, inconsistencies among naming, definition and measurement became noticeable in the relevant literature pool. Some researchers mashed up the definitions and operationalization of the three different designs – willingness, intention, and actual behavior – of SID (see Table 3). Whether or not these inconsistencies are critical is disputable. As already stated, the *intention to behave* can be applied as a substitute for the *actual behavior* of people. Therefore, it is legitimate to define the construct as *disclosure behavior* and in the end measure the *intention to disclose* (e.g., Son and Kim 2008; Wakefield 2013). Still, it is harder to find a scientific legitimation to define the construct as an *intention to behave* or *actual behavior*, which includes the probability, willingness, and likeliness to disclose sensitive information, but in the end *'only'* measures a mere fraction of the construct – namely the *willingness to disclose* information (e.g., McKnight et al. 2002, Metzger 2004). Another scenario that can be discussed in this view on SID is that some researchers are not straightforward in their definition of the construct. In some cases, the construct is named and measured in the correct way, but the definitions are either missing or differing. An explanation for both previously described constellations could be that the words 'willingness' and 'intention' are often applied as synonyms. Nevertheless, since there are differences apparent in the conceptualization of all three designs, distinctions should be made. It can be concluded that there are contributions in which *willingness to disclose* or *actual disclosure behavior* is treated as a substitute of *intention to disclose* and vice versa. For some of these constellations, valid argumentations can be found – *actual*

behavior and *intention to disclose*. Other constellations – e.g., defining the construct as *intention* but measuring the *willingness* – are rather creating a certain fuzziness regarding the understanding of what researchers planned to measure.

In addition to this, SID was operationalized as a one- or multi-dimensional construct with different specifications of 'sensitive information'. It was either specified as a general aspect or as a distinct aspect with multiple information items. Research that specified information into distinct types used this approach to either evaluate causal models with different sensitive elements (e.g., Dinev and Hart 2006; Hui et al. 2007) or to gain more insights on behavioral differences when disclosing on the Internet (e.g., Anderson and Agarwal 2011). Nevertheless, it was found that this approach only makes sense when information items differ from each other. For instance, asking for different health information does not lead to different results in sensitivity, as people perceive all health information as similarly sensitive (Agarwal and Anderson 2011). However, using health information and financial information as distinct types of sensitive information might lead to differences in the observation (e.g., Anderson and Agarwal 2011; White 2004).

Even though there are many different strategies by which to examine the construct, the main findings are similar: people disclose sensitive information, be it generic sensitive information or distinct information items, when the trade-off between the associated benefits (e.g., trust, enjoyment, relationship maintenance, or customized offerings) and costs (the perceived privacy risks or concerns) of disclosure are to the advantage of the benefits. This basic approach stems from the Privacy Calculus Theory (Dinev and Hart 2006), which is grounded in the Social Exchange Theory (Homans 1958). Both theories are predominant in the research on SID in IS and have a focus on an individual's engagement in a decision process to evaluate benefits and costs related to disclosing information (Anderson and Agarwal 2011). Furthermore, it is common to complement this approach with additional social and psychological perspectives to better understand influencing factors on the weighing of costs and benefits. Researchers mainly supplemented trust aspects (e.g., Trust-Risk Framework), which indicates that trust plays a significant role when examining people's willingness to offer sensitive information into IS. Personality traits, trust in an online vendor or SNS users, and sensitivity of information were identified as key influencing factors of the calculus of costs and benefits. Moreover, social science theories, such as the 'Social Capital Theory' or 'Social Penetration Theory' were also in the focus of research to investigate the impact of different social and human interaction aspects (see Table 5).

Besides benefits and privacy topics, some publications focused on trust in particular and its impact on online information disclosure (McKnight et al. 2002; Metzger 2004; Schoenbachler and Gordon 2002). They confirm the assumptions from Privacy Calculus Theory that trust in the online company has a significant impact on the willingness to provide sensitive information to a website (Metzger 2004; Schoenbachler and Gordon 2002). From the SET and trust literature perspective, people who trust in their relational counterpart tend to disclose more personal

information, since higher degrees of trust reduce the risks and concerns related to the revelation of sensitive information. In addition, few studies focused on the impact of specific influencing factors, such as cultural aspects, past experiences, privacy policy transparency or individual characteristics (see Table 6).

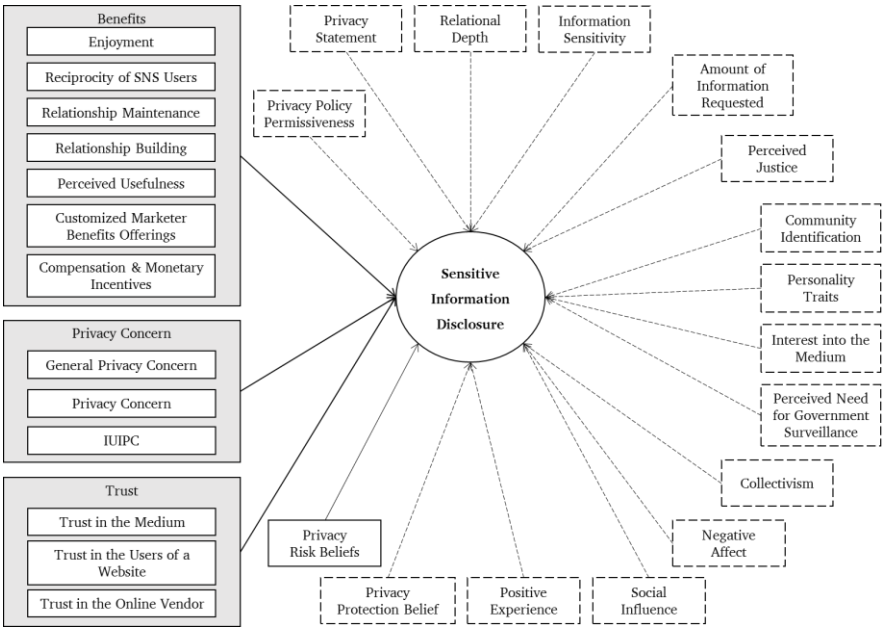


Figure 3: Overview of Influencing Factors on *Sensitive Information Disclosure*

- - - - → Dotted lines indicate a weak relationship (e.g., has not been confirmed through several studies)

——→ Solid lines indicate a strong relationship through repeated studies

Figure 3 shows the results of the exhaustive literature review on the influencing factors on SID in IS and their strength of impact on SID. In this case, the strength describes the amount of research that has been conducted for each construct. Research on SID was primarily focused on influencing factors that stem from Privacy Calculus Theory, but was also complemented with several other influencing factors, for example, concerning personality traits, the social environment, privacy assurances on behalf of the IS provider, or the type of information requested (see Figure 3).

Privacy concerns, as well as privacy risk beliefs, influence a user's SID in a negative way, whereas privacy protection beliefs reflect a user's view about the good intention of a company to protect their provided information against harm and therefore have a positive effect on SID (e.g., Bansal et al. 2010; Hui et al. 2007; Wakefield 2013). Additionally, perceived benefits from disclosure also contribute to the revelation of sensitive information in IS. Furthermore still, if users see that (permissive) privacy statements and policies are published by website companies, the tendency

to disclose is even higher than without this assurance of privacy protection intentions (Gerlach et al. 2015; Hui et al. 2007). This is also the case for the perception of justice: for people who perceive that companies treat provided information fairly and justifiably, readiness to reveal sensitive information increases (Son and Kim 2008). Nevertheless, the higher the sensitivity of information and the amount requested, the fewer people are willing to contribute. Moreover, experiences from the past, such as negative affect, positive experience, and relational depth with a website do influence the decision process of whether to disclose or not. With regard to SNS, community members are more willing to disclose sensitive information if they live in a collectivistic culture (Posey et al. 2010) and can identify themselves with the community (Chen and Sharma 2013). External factors, not directly related to a website or company can also have an impact on the decision process. For instance, personality traits (Hollenbaugh and Ferris 2014) or the influence of the social environment (Posey et al. 2010) can push people to either disclose or withhold.

Research concerning the main influencing factors – privacy concern and trust – focused on these two constructs from different perspectives. For instance, trust can either be understood as trust in the medium (Anderson and Agarwal 2011; Dinev and Hart 2006), trust in a website provider (e.g., Malhotra et al. 2004; Metzger 2004; Wakefield 2013), or trust in the community members of a social network (Chen and Sharma 2013). Furthermore, privacy concerns are either applied as global privacy concerns (e.g., Li and Sarathy 2007), an Internet user's privacy concern (e.g., Malhotra et al. 2004), or privacy concerns as fear of opportunism (e.g., Dinev and Hart 2006). All of these *privacy concern* approaches define concern for privacy intrusion but with slightly different emphases. For both constructs, research neither excludes nor favors one approach; it mainly depends on the goal of the work and the context in which the research was conducted.

3.4. Discussion of Intermediate Results

The goal of this literature review was to provide rich insights on the latest research on SID in EIS and IS in general in order to better understand the inhibitors and drivers of the readiness of employees to disclose sensitive information in software solutions. The review has shown that there is little to no literature on an employee's willingness to provide sensitive information to enterprise information systems. This is supported by Buettner (2015), who points out that there is a research gap regarding usage intention and disclosure behavior of employees. Furthermore, he argued that the previous research was mainly focused on the benefits for businesses when implementing SNS within their companies and was not investigated from the perspective of the employee and their willingness to participate, which is nonetheless crucial for SNS success. In addition, in privacy research there has been demand for the extension of research focus beyond consumer settings and social networks in order to examine organizational contexts (Bélanger and Crossler 2011; Smith et al. 2011). The findings from these literature observations are motivating for further research in the direction of influencing factors on SID in EIS. For this purpose, the present review helps to provide better understanding of important contributions to the Internet and online context. While the primary focus of researchers is on the trade-off between privacy concerns and risks and on the opposing perceived benefits of exposure, research

has also revealed that information sensitivity, legal regulations, personality traits or cultural differences are significant inhibitors or drivers of SID (see Figure 3 and Table 6). However, central influencing factors are trust in the vendor or online community, perceived benefits (such as relationship maintenance), perceived risks, and privacy concerns related to disclosure on the Internet.

Research considering the enterprise context should investigate whether these decisive aspects are also relevant in the organizational setting when employees are asked to contribute sensitive information in enterprise systems.

3.4.1. Implications

With regard to critical influencing factors on an employee's disclosure behavior in EIS, this study shows that there is a need for research on this topic. The focus of present studies on information disclosure is on public SNS, e-commerce and the Internet in general. The findings of this review provide valuable insights regarding the factors influencing SNS, e-commerce websites, and Internet success by showing when users disclose information. Future empirical research could use the results as a starting point, conducting qualitative or quantitative studies in the context of EIS to better understand if influencing factors of sensitive information disclosure research can also be applied in this regard and to identify possible further dynamics and factors affecting the willingness to disclose sensitive information into EIS. Along these lines, it was found that privacy research is one of the main research streams, focusing on the self-disclosure topic. As companies implement SNS more and more to support collaboration and increase business success, it could be a good starting point to investigate the information disclosure behavior of employees in so-called *Enterprise Social Systems* (ESS) with regard to privacy research.

Furthermore, research has the potential opportunity to find out how specific influencing factors, such as trust or privacy concern should be applied in the organizational context. Both constructs are implemented in different ways in the non-enterprise context, whereas some definitions and operationalization might not be applicable in the enterprise context. This should be clarified in future research, as the relationships between the provider and users of a software solution are of a different nature. Employees might have a more professional relationship with other employees contributing within ESS, as well as to the employer, who is probably the host of the ESS.

Regarding benefits, it can be concluded that not all benefits have the same positive impact on SID in IS. As an example, in e-commerce contexts it is noteworthy that, when offered monetary rewards or compensation in exchange for information provision, consumers might react with information refusal or misrepresentation (Li and Sarathy 2007; Yang and Wang 2009) since they do not want to see their personal information treated as a valueable commodity (Hoffman et al. 1999). This might also be valid for the employer-employee context. When employers want to trade rewards for information, the sensitivity and perceived relevance of the requested information play a significant role, as employees may not want their information to be treated

as an valueable commodity. When employees perceive that the requested information is sensitive and that it is being treated as a cheap commodity, they might refuse disclosure. This fact should be considered when conducting further studies in the context of EIS and privacy of employees. There are missing insights on what really motivates employees to disclose sensitive information in the sense of perceived benefits. Therefore, research should be conducted to find out how companies could incentivize their workforce to make enterprise systems where employees have to disclose sensitive information successful.

3.4.2. Limitations and Further Research

The results underlie limitations that indicate paths for further research. First, adolescent research on self-disclosure was excluded from the research. While this research is critical, I believe that focusing on topic areas closer to the actual context of information disclosure in EIS of employees, who are mainly grown adults, better reflected the behavior. Research on adolescents' SID behavior in SNS does not represent the target group of employees.

Furthermore, research focusing on the comparison of face-to-face and computer-mediated interaction was also excluded from the review. This kind of investigation is mainly focused on the differences between direct and indirect communication with computers and the related changing willingness of disclosure when communicating either face-to-face or through a technological medium. However, this research could offer further insights on the disclosure intention of people in general and might provide an opportunity to further generalize the findings.

In addition, only the most relevant papers and conference proceedings of information disclosure in IS were included in the sample. The sampling was based on the quality of the conference or journal and the number of citations (VHB-JOURQUAL 3 Ranking). The less relevant contributions were, however, also screened on the surface to make sure that no possible trend was missed and a deep analysis of those contributions could also help to gain further insights on SID of people both in general and in the employee context.

4. Sensitive Information Disclosure in Enterprise Social Systems – A Qualitative Study

4.1. Introduction

The topic of users' information disclosure in social networking systems (SNS) and e-commerce websites has been heavily debated among both academics and practitioners. As shown in the previous section (Section 3), research has made valuable contributions to the understanding of the drivers and inhibitors of an individual's tendencies to share sensitive information online (e.g., Dinev et al. 2013; Krasnova et al. 2010; Malhotra et al. 2004; Xu et al. 2011). These significant findings revolve largely around a central theoretical perspective, the Privacy Calculus Theory. It states that a user's information sharing behavior depends on the benefits as well as the privacy risks associated with disclosure (Culnan and Bies 2003; Dinev and Hart 2006; Laufer and Wolfe 1977). Corresponding to the findings of the previous section and to complement the current research on sensitive information disclosure (SID) in enterprise information systems (EIS), a qualitative study investigating the impact of Privacy Calculus related influencing factors on SID in enterprise social systems (ESS) is going to be conducted.

4.1.1. Motivation

Investigations of users' privacy and information disclosure in SNS have as yet been limited to the context of public networks such as Facebook (e.g., Dinev et al. 2013; Gerlach et al. 2015; Krasnova et al. 2010; Xu et al. 2011). This seems surprising given the current relevance of SNS for intra-organizational purposes (Chui et al. 2012). ESS promise numerous advantages such as increased knowledge diffusion, easier collaboration, relaxation of strict hierarchies, or the provision of data sources for big data analytics (Chui et al. 2012; Kügler and Smolnik 2013; Leonardi et al. 2013). As for public SNS, the success of ESS is strongly determined by the information individuals disclose in the system. Apparently, benefits like knowledge distribution or insights through data analytics cannot be achieved if users refuse to share honest information in ESS. This makes it critical for organizations to understand the factors which affect who shares what and why in ESS. Moreover, it has been previously demanded that privacy research should be extended beyond consumer settings and in particular, investigate organizational contexts and behaviors (Bélanger and Crossler 2011; Smith et al. 2011).

Although it seems likely that ESS success and the employee's SID depends on users' privacy perceptions, as this is the case in the consumer context, the significant differences between organizational and leisure settings are distinct as well. First and foremost, social structures are of very different quality in organizations compared to in public SNS. In particular, employees strongly depend on their colleagues, supervisors, or senior management, and thus on the company as a whole. This presents a fundamental difference when compared to a user's relation with a provider of a public SNS. For most employees whose jobs are a central part of their lives, this makes information disclosed in an ESS a more delicate matter compared to a public third-party platform. Risks that emerge from such sensitive information disclosure might be perceived as being far more immediate and tangible as those associated with public SNS, which are often

said to be rather vague (e.g., Smith et al. 2011; Wilson and Valacich 2012). Moreover, the employee's technology use might be associated with their performance evaluations, which leads to questions regarding the correctness of information disclosed. Several other factors differentiate the organizational context from public social networks, such as the employee's duties during work hours or the corporate trust culture.

4.1.2. Derivation of Research Questions

Given these considerations, it can be argued that IS research on privacy and sensitive information disclosure in ESS should be conducted to complement previous findings in the consumer and social context. Therefore, this subsection deals with the following research question:

How do privacy factors and organizational factors influence employees' beliefs about enterprise social systems and thus, their sensitive information disclosure behavior?

An interpretive case study was conducted in a globally operating company to answer this question. This interpretive approach was deliberately chosen since the aim was to evoke an open-minded discussion about individuals' needs, concerns, and ideas, as well as the peculiarities of the organizational context. Several interesting effects could be discovered which significantly improve the understanding of the determinants and outcomes of ESS use. Thereby, it could be identified that the Technological Frames Theory can serve as highly valuable framework considering the particular employer-employee context in which ESS are used as opposed to public SNS. The results contribute to theory, as they show a first attempt to extend the research on sensitive information disclosure in SNS toward organizational social network systems, and offer an initial idea on how the corporate environment and setting could influence ESS success. Furthermore, the findings provide insights for managerial practice regarding what aspects have to be considered when companies aim to implement ESS or minimize failures successfully.

4.2. Basic Definitions

In this subsection, the central constructs of this research are going to be defined and explained in detail. An overview of ESS, its functionalities, and the related term Enterprise 2.0 will be given. In addition, information privacy, information privacy concerns and information privacy risk beliefs are going to be outlined.

4.2.1. Enterprise Social Systems & Enterprise 2.0

Enterprise 2.0 refers to the phenomena of a participative organizational culture regarding communication and information exchange with social software technologies (Richter and Riemer 2009) and is defined as *'the use of emergent social software platforms […] by an organization to pursue its goals.'* (McAfee 2011, p. 1). Enterprise 2.0 adopts principles and information technologies of Web 2.0 and focuses on user collaboration and collective content creation by all participants (Hacker, Bodendorf, and Lorenz 2016). Research on Enterprise 2.0 does not only focus on the usage and implementation of social software, but rather describes a broad concept on how a culture of employee participation, integration, and mutual usage can

be established and supported by software (e.g., Buhse and Stamer 2008; Kügler, Smolnik, and Kane 2015; Leidner, Koch, and Gonzalez 2010). Nevertheless, when discussing social software in enterprises, it can be referred to by use of various similar or even substitutable terms. As for instance, Enterprise Social Systems (Alimam, Bertin, and Crepi 2015), Emergent Social Software Platforms (McAfee 2013), Enterprise Social Media (Leonardi et al. 2013), or Enterprise Social Networks (Hacker et al. 2016). In this research, the term ESS will be adopted, as it underlies their systemic nature (Alimam et al. 2015), which is relevant for this research. In general, ESS have the goal to combine social relationships with enterprise processes and activities (Buregio, Maamar, and Meira 2015). Furthermore, Leonardi et al. (2013) defined two goals that ESS focus on: first, *collaboration and support for teaming up* by aligning actions and interactions among stakeholders, and second, *social support* by connecting employees around mutual interests or tasks. Examples for ESS reach from SNS-like internal networking tools to company internal blogs, expert networks, wikis, skill databases, or employee profiles (Alimam et al. 2015; Chui et al. 2012). In this research, ESS refers to tools that offer an opportunity for users to connect with each other, form communities, and share user-created contents within a company (DiMicco et al. 2008; Kim, Jeong, and Lee 2010).

4.2.2. Information Privacy

With regard to the research context, it is important to understand how information privacy is defined and conceptualized. Therefore, this subsection describes where information privacy comes from and how it is understood today.

As Westin (2003) has already mentioned, privacy is a *'fundamental part of civil liberty in democratic society'* (Westin 2003, p. 434). Hence, privacy is a social good in democracy and focuses on the rights of individuals to decide when they want to speak, disclose, love or enter into a relationship with someone (Westin 2003). Furthermore, privacy has been understood as a legal or moral right (see Bélanger and Crossler 2011) or as an individual's ability to control personal information (Bélanger et al. 2002; Stone et al. 1983). Information privacy is a specification of the larger concept of privacy which has been studied and examined for ages (Bélanger and Crossler 2011). Since today communication and information technologies drive a lot of privacy concerns by collecting, analyzing and aggregating information faster and in a larger volume, the focus of privacy research is shifting more and more in the direction of information privacy (Bélanger and Crossler 2011). These privacy concerns are described as the loss of control over secondary usage of personal and private information (Bélanger et al. 2002), with secondary usage referring to the practice of using information for other purposes than that which the data was collected. As the present study is concerned with the employee's sensitive information disclosure in ESS and their related fear about information privacy, it is defined as '*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*' (Westin 1967, p. 7).

4.2.3. Information Privacy Concerns

Not only is information privacy – as a right of an employee to decide when and where to disclose his information – important, but also his related concerns when communicating sensitive information. Those concerns are mainly studied as perceived consequences of SID (Xu et al. 2011). IS research has further referred to information privacy concerns as *'concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular'* (Dinev and Hart 2006, p. 64). In the present context, this would mean that employees worry about the opportunistic behavior of their employers when introducing sensitive information into ESS. These concerns might stem from the fact that they do not know how their company might use the entered information and from fear of behavior that only considers the employer's needs and not those of the employee himself. When this definition is adapted for the present context of ESS and the employer-employee relationship, it results in the definition of privacy concerns as *concerns about opportunistic behavior by the employer related to the sensitive information submitted over an ESS.*

4.2.4. Information Privacy Risk Beliefs

In IS research, 'privacy risk beliefs' were identified as one of the main negative influencing factors on SID (e.g., Dinev and Hart 2006; Krasnova et al. 2010; Malhotra et al. 2004). The perception of risk is related to the uncertainty of an Internet user concerning the fear that revealing information to a website or seller might result in a loss for the user (Dinev and Hart 2006). The difference among 'privacy risk beliefs' and 'privacy concerns' is that privacy risk beliefs describe the fear of loss when disclosing information, whereas privacy concerns outline a general concern about opportunistic behavior not directly related to a feeling of loss. Therefore, IS research has further referred to information privacy risk beliefs as the *'expectation that a high potential of loss is associated with the release of personal information to the firm'* (Malhotra et al. 2004, p. 341). Transferring privacy risk beliefs into the present context, this would mean that employees perceive a high potential for loss when disclosing sensitive information in ESS. When adapting the definition to the current scenario, privacy risk beliefs are defined as *the expectation that a high potential for loss is associated with the release of sensitive information to the employer* (based on Malhotra et al. 2004).

4.2.5. Overview of Definitions

All in all, it can be said that the employee's perceptions of how their inserted sensitive information in ESS is potentially processed by their employer and how their fears of privacy loss influence their beliefs and behaviors regarding ESS will be investigated. The following table (Table 7) gives an overview of the relevant constructs and the related and developed definitions of the previous subsection:

Construct	Definition
Enterprise Social Systems (ESS)	*Tools that offer an opportunity for users to connect with each other, form communities, and share user-created contents within a company* (based on DiMicco et al. 2008; Kim et al. 2010).
Information Privacy	*'The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'* (Westin 1967, p. 7).
Information Privacy Concerns	*Privacy concerns are concerns about opportunistic behavior by the employer related to the sensitive information submitted over an ESS* (based on Dinev and Hart 2006, p. 64)
Information Privacy Risk Beliefs	*Information Privacy Risk beliefs refer to the expectation that a high potential for loss is associated with the release of sensitive information to the employer* (based on Malhotra et al. 2004, p. 341).

Table 7: Overview of Definitions

In light of these definitions, the following qualitative research will investigate the employee's perceived right to control when, how and to what extent he wants to communicate information about himself in ESS. Furthermore, his related concern of the employer's opportunism and belief about a potential loss associated with the disclosure of information will be investigated. ESS offer the employee a possibility to connect with other employees, form communities, or share employee-created contents within his company.

4.3. Theoretical Background

With regard to the research topic, two research areas are going to be introduced. To get an overview of how the issue of privacy has been handled in the past by information systems literature, the first part of this section gives an overview of the present studies on privacy research in IS literature. Furthermore, to build an understanding of the research context and how to embed privacy in the ESS environment, an overview of the already existing research on the employee's usage of ESS is given in the second part of this section. Additionally, the theory of Technological Frames will be introduced, which serves as a fundament for further research.

4.3.1. IS Privacy Calculus Research

This section aims at providing a brief overview of the literature on the individual's information sharing behavior in SNS and IS in relation to Privacy Calculus Theory. Exhaustive reviews and overviews on privacy in general already exist elsewhere. For instance, Bélanger and Crossler (2011) provide a comprehensive literature synopsis on information privacy literature in IS. Moreover, an interdisciplinary review of the literature on information privacy concerns was conducted by Smith et al. (2011). As the research of this section focuses on the Privacy Calculus Theory and its constructs as influencing factors on SID, this theory, and the identified phenomena will be at the center of this review.

The calculus perspective on information privacy understands a person's interests in privacy as an exchange between an individual's sensitive information and certain benefits (e.g., Dinev et al. 2009; Xu et al. 2011; Gerlach et al. 2015; Krasnova et al. 2010). Research evolved around the idea that an individual's willingness to share sensitive information or to transact over the Internet is influenced by the perceived costs and benefits of disclosing information (for more information see Section 3). The trade-off – called Privacy Calculus – is significant for specifying and interpreting an Internet user's behavioral intentions (Smith et al. 2011). This economic perspective on privacy suggests that when someone is asked to provide personal information to another party, the provider assesses the risks and benefits of disclosure to analyze the possible outcomes he could face when offering information and reacts accordingly (Dinev and Hart 2006). On the negative side, privacy risks and concerns reflect the belief that there is a high potential of loss when releasing information to someone (Malhotra et al. 2004) and prevent people from disclosing sensitive information. On the positive side, perceived benefits, – for example, the enjoyment or forming social relationships – encourage people to disclose (Krasnova et al. 2010). In addition, trust beliefs, reflecting the expectations of a trustor that a trustee behaves predictably, fulfills his commitments, and acts fairly (Chen and Sharma 2013), have been shown to facilitate SID (McKnight et al. 2002). When assessing these beliefs against each other, the IS user believes himself to deliberately manage their SID behavior. In former research rich evidence is provided for the applicability of the Privacy Calculus Theory to the SNS context. For instance, Koroleva et al. (2011) empirically revealed that entertainment, as well as social adjustment, enhances the disclosure of information by teenage users, whereas the awareness of privacy and information availability leads to restricted information disclosure. Furthermore, Krasnova et al. (2010) showed that the role of trust, privacy risk perceptions and multiple benefits influence SID decisions of SNS users. Overall, when considering the Privacy Calculus Theory trust, benefits, privacy risks, privacy concerns, and information sensitivity play a crucial role in the decision-making process of whether to insert sensitive information into software solutions or not (e.g., Dinev et al. 2009; Dinev and Hart 2006; Gerlach et al. 2015; Krasnova et al. 2010). In the following, these factors will be described in more detail.

Privacy Risk and Concerns. Privacy risk and privacy concerns alike are risk beliefs, while the latter is an internalization of the possibility of loss. Dinev and Hart (2006) describe privacy risks as a belief which amounts to the assessment of websites in general, and privacy concerns as a valuation about what is happening to sensitive information of Internet users when disclosed. Hence, perceived risks and perceived privacy concerns are related to each other but are nevertheless distinct factors to measure and investigate. When measuring privacy risk beliefs, the potential of loss when releasing personal information to someone is investigated (Dinev and Hart 2006). Privacy Calculus researchers have identified the provision of sensitive information to third parties, unauthorized access or identity theft as sources of perceived risks (e.g., Dinev and Hart 2006; Gross and Acquisti 2005). Furthermore, the assessment of risk includes the evaluation of the probability of negative outcomes and the perceived seriousness of the related consequences, which have an impact on an individual's emotions, decisions, and physics (Smith et al. 2011). Consequently, a number of studies on the Privacy Calculus have focused on the

willingness of customers to transact on e-commerce website as related consequence (e.g., Li and Sarathy 2007; Li et al. 2011; Pavlou and Gefen 2004), the impact of perceived privacy risks on the information disclosure behavior (e.g., Malhotra et al. 2004), and how privacy risks generally increase privacy concerns (e.g., Dinev and Hart 2004).

Privacy concerns reflect worry about opportunism on behalf of the employer when submitting information into information systems (Dinev and Hart 2006). It refers to the fear that submitted information might be misused or used in a way that was not foreseeable by the provider of the information. Findings in the literature show that these concerns have an impact on an individual's attitude (Dinev et al. 2008; Milberg, Smith, and Burke 2000). Foremost, privacy concerns influence the readiness of people to disclose information on websites (Anderson and Agarwal 2011; Krasnova et al. 2012; Li et al. 2011; Malhotra et al. 2004; Son and Kim 2008). As already described and discussed in Section 3.2.3, Privacy Calculus literature examines and assesses privacy concerns from different perspectives. In general, the basis of the construct stems from Smith et al.'s (1996) research on the Concern for Information Privacy and the Social Contract Theory (Malhotra et al. 2004). Smith et al. (1996) developed the 'Concern for Information Privacy' to measure a person's concern about companies' information privacy practices in the direct marketing context (Malhotra et al. 2004), where the collection, errors, unauthorized secondary use and improper access to provided information are the central dimensions of privacy concerns. Malhotra et al. (2004) introduced the dimensions of *awareness* and *control* from Social Contract Theory because they believed that in the Internet context, those dimensions conveyed the concerns about the company's privacy practices. Therefore, the construct describes a person's perception of fairness or justice in the context of information privacy when disclosing information in online scenarios.

As the present context also deals with the disclosure of sensitive information and literature shows that both constructs have an impact on the disclosure behavior, they might also play a decisive role in the decision of employees whether to disclose in ESS or not. However, the sources of privacy risk beliefs and concerns might differ, since the social structures within a company are of a different quality compared to SNS. There might be a direct dependent relation between employees, their supervisors, co-workers or the senior management of the company, which could have an impact on privacy risk beliefs or privacy concerns.

Perceived Benefits. Related to the concept of the Privacy Calculus, perceived benefits are an employee's belief about the extent to which he or she will become better off from providing information (based on Kim, Ferrin, and Rao 2008, p. 547). Hence, perceived benefits of the usage of a software system lead to increased information disclosure, as people hope to perceive a positive outcome. In general, researchers identified financial rewards (e.g., Phelps et al. 2000; Xu et al. 2010), personalization options (e.g., White 2004), enjoyment (e.g., Krasnova et al. 2010; Wakefield 2013) and social paybacks (e.g., Krasnova et al. 2010) as the main advantages associated with disclosing information. In the relevant SNS literature, researchers revealed that the value of relationship building and maintenance influence the intention to disclose

information significantly (e.g., Krasnova et al. 2010; Hollenbaugh and Ferris 2014). Furthermore, simple enjoyment of an SNS also contributes to the willingness to disclose (Wakefield 2013). Literature shows that various perceived benefits, depending on the context and software system/website in focus, have an impact on the disclosure behavior of people. In the present context, the same might be true. Any perceived benefit from disclosure might have a positive impact on the actual willingness of employees to participate in ESS and in turn might decrease their perceived risks and concerns.

Trust. Trust in Privacy Calculus literature is mainly seen as a counterpart to privacy risks or concerns. More reliable companies will have a competitive advantage (Bowie and Jamal 2015). Moreover, researchers have revealed that it is more efficient to employ trust building measures than to try to reduce privacy concerns (Milne and Boza 1999). For instance, privacy seals (LaRose and Rifon 2007), clear communication of privacy policies (Andrade, Kaltcheva, and Weitz 2002) and the application of privacy protocols (e.g., P3P) (Xu, Teo, and Tan 2005) were found to be helpful as trust building measures. In the present context, this might indicate that employers who are more trustworthy could have a higher resulting benefit from investing in trust measures than in measures against the employee's privacy concerns.

Information Sensitivity. With regards to privacy, the types of information that are asked to be disclosed play a decisive role in the decision process of whether to reveal or not (Dinev and Hart 2006; Phelps et al. 2000; Yang and Wang 2009). When it comes to the degree of sensitivity, lifestyle characteristics are weighted as less sensitive than personal or private information (for more information see subsection '2.1.2 Sensitive Information'). Several researchers found a statistically significant direct impact of sensitivity of information on the behavioral intention of people (e.g., Malhotra et al. 2004; Xu et al. 2008). Hence, people perceive the severity of privacy risks and concerns depending on the perceived sensitivity of the requested information. As in ESS different types of information might be requested from the employee, the same could hold true for the research context of this dissertation.

This study addresses information privacy of employees in the company setting. Therefore, it should be noted that privacy concerns and risks might be of a different quality in an organizational setting as they do not involve usually mentioned aspects like improper access (e.g., identity theft) or secondary usage (e.g., selling of data). In organizations, possible risks and concerns might arise as a result of users' dependencies on the employer and could range from unfavorable evaluations to layoffs. Furthermore, since the job is often seen as a central part of an employee's life, it makes information disclosed to an employer a potentially more delicate matter than in leisure contexts.

4.3.2. Employees' Enterprise Social System Use

The increasing importance of ESS has been exhaustively discussed among researchers (e.g., Kügler et al. 2015; Kügler, Smolnik, and Raeth 2012; Raeth, Kügler, and Smolnik 2011), and the implementation and usage have become pervasive within companies (Leonardi et al. 2013).

Furthermore, research has shown that ESS exert powerful effects on the way internal collaboration takes place and how companies communicate and interact with external stakeholders (McAfee 2006). Although ESS have received increasing attention in recent years, research regarding antecedents and outcomes of effective ESS use is still sparse. Nevertheless, a few studies examining the use of ESS among employees exist (e.g., Herzog et al. 2013; Kügler and Smolnik 2014; Larosiliere and Leidner 2012; Wattal et al. 2010).

While these studies provide promising first insights, their majority are focused on measuring the success of ESS usage. As a valuable starting point, Kügler and Smolnik (2014) propose a conceptualization of usage modes for ESS. Along these lines, Herzog et al. (2013) examined the success of ESS by analyzing the methods and metrics applied by organizations, which served as measures for the usage of ESS by employees. Kügler and Smolnik (2013) investigate the benefits associated with ESS use for employees. The authors propose that ESS can increase employees' efficiency, affect their connectedness, support decision-making performance, and also increase innovative performance. In the same vein, a study regarding organizational Facebook use showed that organizational identification can be increased through ESS use by the organization's members (Larosiliere and Leidner 2012). Furthermore, Buregio, Maamar, and Meira (2015), as well as Williams et al. (2013), identified potential benefits and risks for companies and employees when using ESS. For instance, ESS enable quicker resource access but can simultaneously cause an overload of information (Buregio et al. 2015).

Research on the adoption of ESS aims to identify best practices and factors that influence the end-user adoption of ESS (Alimam et al. 2015). Regarding possible antecedents of ESS use and acceptance, Kügler et al. (2012) provide a first draft of a theoretical framework on how the acceptance of ESS could be examined. The authors suggest that the use of ESS might be influenced by organizational climate as well as by social and technical factors. Wattal et al. (2010) examined the use of organizational blogs by employees and found that network externalities and feedback from other users as recognition are crucial for the motivation to use enterprise blogs. Even though previous IS research irrevocably showed that privacy concerns are a major influencing factor for the provision of personal information in SNS, there is a lack of research on this phenomenon in the organizational context.

In sum, extant research on organizations' implementation of ESS and the employee's use thereof has largely focused on outcomes of these systems (e.g., Herzog et al. 2013; Kügler and Smolnik 2013; Larosiliere and Leidner 2012). However, it is necessary to understand the reasons for and origins of the employee's privacy concerns about ESS, and thus the success factors for such technologies within organizations. As will be outlined below, incongruence in technological frames between employees and their employer play a central role in understanding the employee's beliefs about ESS, and thus their behavioral consequences and demands toward the company.

4.3.3. Technological Frames as Conceptual Framework

Early throughout the data collection of this study, an emergent pattern could be recognized. Despite an open-minded outset, employees' perception of the implementation purpose of ESS differed from the employer's actual intent. Thus, as a better impression of the collected interview data was obtained, the Technological Frames Theory as the conceptual model for the present study became more and more evident (Walsham 2006). It serves as a theoretical structure focusing on technological frames of reference to examine interpretations associated with organizational IT. The concept of technological frames is used in research to better understand the adoption decision and user perceptions of technologies (e.g., Angst and Agarwal 2009; Lin and Silva 2005; Mazmanian 2013; Mishra and Agarwal 2010). Technological Frames represent cognitive structures by which users of technology understand the position and role of technology, its usage, and the effects and consequences resulting from usage (Orlikowski and Gash 1994).

The Origin of Technological Frames

The fundamental work for technological frames was conducted by Orlikowski and Gash in 1994. They developed a conceptual framework which builds the cornerstones of the socio-cognitive research on information technology. They concluded that people of a particular social group have similar understandings of technologies and its artifacts. This research is concerned with the cognitive structures held by different groups in an organization toward end-user computing. Orlikowski and Gash's basic argument explaining the relevance of technological frames as a theoretical view in IS research was the premise that humans behave on the basis of their subjective understanding of their environment (Berger and Luckmann 1967; Weick 1979), with these interpretations being incorporated into the context of technologies in companies.

The Characteristics of Technological Frames

Orlikowski and Gash (1994) defined technological frames as *'that subset of members' organizational frames that concern the assumptions, expectations, and knowledge they use to understand technology in organizations. This includes not only the nature and role of the technology itself, but the specific conditions, applications, and consequences of that technology in particular contexts'* (p. 178). They set the basis for a variety of research on technological frames by identifying three main domains characterizing the interpretations of the technology in focus and its role in the company (e.g., McGovern and Hicks 2004; Olesen 2014; Shaw and Ang 1994; Yoshioka et al. 2002). The first domain was the *nature of the technology*, which is related to the view of people on the system and the understanding of the abilities and functionality of the solution. Second was the *technology strategy*, including the people's images of why the employer has acquired and implemented an IS. It refers to the understanding and interpretation of what has driven the decision to adopt the system and its related value for the employer. As a third domain, they identified the people's interpretation of how the *technology is used* in the day-to-day business, along with the settings and outcomes linked with this usage (Orlikowski and Gash 1994).

These three aspects help to foster conclusions about the different perceptions of technologies and the related usage from various stakeholder groups. Therefore, frames not only exist on the level of individual people, but also on the social group level where individuals within the group share common technological frames which direct their interpretations, understanding and usage behavior with the related technology (e.g., Davidson and Pai 2004; Olesen 2014). In their empirical study, Orlikowski and Gash (1994) identified three main social groups in companies that have different technological frames for IT – namely, the *technologists* who execute the implementation of the enterprise system, the *user group* of the system, and the *manager group* which decides if the technology should be adopted. The primary focus of technological frames research is on the upcoming problems when frames of relevant social groups are different and are therefore incongruent (Orlikowski and Gash 1994). This incongruence of frames of the organization's important stakeholder groups indicates significant differences in presumptions, expectations, or knowledge about several key characteristics of the related technology and can result in significant consequences for the success of an IS. For example, frame incongruence is recognizable when users think that technology is provided to only make the employer work harder and faster and control their behavior, while managers expect the technology to change the way their organization is doing business (Orlikowski and Gash 1994). On the other hand, congruence in technological frames would indicate that people in social groups have similar expectations about the impact and role of the technology in business decisions, the means of usage, or, for example, the type and regularity of the technology's support and maintenance. Therefore, Orlikowski and Gash (1994) defined the notion of congruence in technological frames as *'referring to the alignment of frames on key elements or categories. By congruent, it is not meant identical, but related in structure (i.e., common categories of frames) and content (i.e., similar values on the common categories)'* (p. 180). When there is incongruence, it may result in wrong expectations, inconsistent actions, resistance, suspicion, and limited use of the technology. The central interest of Orlikowski and Gash was to interpret IT and organizational change with the application of technological framing. In particular, they aimed to understand the costs arising from incongruent frames and suggested that awareness and related interventions could help to overcome this incongruence and to bring different frames within an organization into line.

For the research of this section and the related research questions, the Technological Frames Theory serves as the structure for the employee's interpretations about ESS and the influencing factors on their willingness to use the technology by disclosing sensitive information. Moreover, it helps to explain the reason why employees do have different perceptions on ESS than their employers and what consequences are behind it. The main goal of the application of the theory is not to elaborate on the incongruence of frames and give implications on how to align those frames, but rather it will help to structure the analysis of the qualitative data and to better understand the fundamental issues and challenges that employees have when it comes to the usage of ESS. Besides, recent studies on technological frames suggest the need to look beyond the organizational borders and to include environmental and cultural aspects into the analysis (e.g., Davidson 2006), which will also be a subject of this research.

4.4. Frame of Reference of the Study

Accordingly, in this study, the goal is to understand how employees perceive the technological frame of ESS, including the three dimensions of *strategy*, *usage*, and *nature* in the ESS technology. Furthermore, the goal is to find out what the consequences and the demands of employees toward their employers are as a result of using these systems. The research is conducted with regard to previous Privacy Calculus Research, which has had a massive impact on the knowledge gain on SID in SNS (see Section 3). It serves as the fundamental source of inspiration on possible influencing factors on SID in ESS.

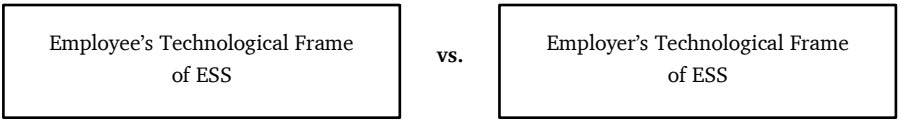


Figure 4: General Frame of Reference of the Study

Figure 4 and Figure 5 give an overview of the frame of reference of this qualitative study and at the same time explain the structure of subsection *'4.6 Case Study Results*', where the study outcomes are analyzed. The analysis is divided into three main parts. First, the incongruence of the technological frame between the employee and employer representatives will be analyzed and illustrated (Figure 4). Afterwards, the employee's technological frame will be reviewed and analyzed in detail. Therefore, the three characteristics of the technological frames perspective will be examined for the employee in the present scenario (Figure 5). Therefore, (1) the employee's perception about the ESS strategy, (2) how he uses ESS and (3) the nature of the technology in use will be analyzed and explained in detail. In the end, the employee's expectations and his behavioral consequences resulting from the frame incongruence with his employer will be compiled.

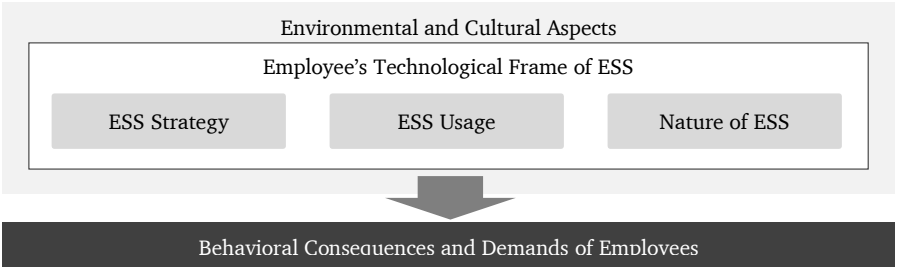


Figure 5: Detailed Frame of Reference of the Study

4.5. Methodology

Considering the delicate nature of employees' perceived privacy when using ESS in organizations, a purely positivist approach including a predefined set of constructs and hypotheses would not do justice to this largely unexplored context. Instead, it should be fruitful

to listen to the nuances of employees' concerns, needs, and backgrounds in a more exploratory manner. Therefore, an interpretive approach has been chosen to study the topic (e.g., Klein and Myers 1999; Walsham 2006). The interpretivist stance thereby assumes that human agents socially create the reality. Therefore, the goal of an interpretive approach should be to understand the interpretations of phenomena and situations by the informants (Klein and Myers 1999; Walsham 2006) and to challenge existing theories with new circumstances and contexts (Walsham 2013). Since the research of this section investigates how organizational factors influence the employee's beliefs about ESS and thus their willingness to disclose information in ESS, case studies are the favored approach when such questions are asked (Yin 2011).

4.5.1. Case Description

The case study was conducted in a large company with headquarters in Europe (all names are pseudonyms), employing more than 10.000 people globally. This organization was explicitly chosen as the case company for the provision of a particularly interesting constellation. Historically, the company's corporate culture was rather liberal in nature. Employees were provided several advantages like sport and leisure time activities on the company campuses, flexible working hours, and home offices without control mechanisms like time clocks or performance records. Moreover, the company had already installed a wide range of ESS throughout the organization (e.g., communities, collaboration systems, closed discussion groups, social search). Seven years ago, for example, the company implemented a social collaboration system within the enterprise to provide employees an environment in which they could find, connect, collaborate, and learn from each other. The company's intention with the system was to enable the workforce to diffuse relevant information about their work and each other, and furthermore to develop connections with employees around the globe. Despite an open and informal company culture, however, the overall usage extent for many of these social systems was rather poor.

Data collection was aimed at obtaining insights about the constellation described above by interviewing affected employees. Rather than measuring levels of agreement or disagreement about such systems, the goal was to gather a range of perspectives regarding the employee's reasons for using or not using ESS. It was assumed that sensitive information disclosure in these systems should correlate with increased knowledge of IS (e.g., Li 2011) as well as with participants' age (e.g., Malhotra et al. 2004). Theoretical sampling was applied to obtain a rich impression along these lines. Therefore, respondents of different ages were chosen from R&D versus more business-related departments of the company (i.e., HR or consulting). To set these participants' opinions into perspective, (senior) experts from HR were interviewed to elaborate on the company standpoint. All in all, the set of respondents comprised 21 people with an average age of 38. Five interviewees were younger than 30; seven interviewees were between 30 and 40, and eleven interviewees older than 40. The youngest participant was 25 years old; the maximum age was 55. Three were female and eighteen were male. As assumed, R&D workers had significantly higher IT-related knowledge than those with business backgrounds according to t-tests conducted on corresponding questionnaire data (group means = 6.4 vs. 4.9, $p < 0.01$).

Departments	Number of Interviews
R&D Department (IT background)	11
HR Department, Consulting (business background)	7
HR Experts (organizational perspective)	3

Table 8: Overview of Participants

Primarily, interviews were conducted with European employees of the company. For a better generalization of the study results, however, four of the interviews were held with American representatives of the organization. Table 8 illustrates the departments of the participants and the respective numbers of interviews.

4.5.2. Data Collection

The data was collected by conducting semi-structured interviews to allow for systematic assessments across the respondents (Myers and Newman 2007). Both data collection and the subsequent analysis were thereby guided by the set of principles for interpretive field studies, suggested by Klein and Myers (1999). For a shared understanding among all participants and thus comparable results, a list of tools and functionalities (i.e., what is understood as ESS) was provided before each interview (Table 9).

Functionalities	Example Information
Personal profile	name, location, job, organizational chart, company membership, cost center, telephone, manager, mail, assistant
Skills and knowledge	team specific skills, Line-of-Business skills, soft skills, technical skills, languages
Prior Experience	previous work [internal and external], education
Connect with coworkers	build a network
Blogs with comment function	organization-wide blogs where employees can discuss several topics, such as organizational strategy, workplace, innovation or products of the company
Expert Finder	find experts based on their job description, skills, and knowledge
Groups	build groups to discuss with specific target groups
Status updates	provide an update on what you are doing or feeling
Feeds	news feeds about happenings in the company
Liking	like other posts and comments
Chat and Direct Messages	directly contact peers and managers through a social network

Table 9: List of ESS and Example Information

A coarse interview protocol was prepared for discussion with the interviewees (see Table 10). The overarching idea of the protocol was to find out which meanings employees associated to ESS as well as antecedents and consequences of these beliefs. Nevertheless, employees were welcomed to elaborate on their own considerations. Therefore, appropriate deviations from the protocol were accepted.

Semi-Structured Interview Guide	
Sensitive Information:	Which functionality of the system would you use? Why?
	What kind of data would you disclose in the systems? (Enhanced data, like skills so someone can benefit from your knowledge?) Why/Why (not)?
	Would it change your opinion when… …the company forces you to use the system? …when you would know that your data is used for predictive analysis and enriched with other personal information?
	Would you behave differently in a social system not hosted by your company?
Influencing Factors:	If you would have to disclose data into a system hosted by your company, what would harm/motivate you to do that?
	Are there factors that are more important to you than others? Why?
Trust:	Do you trust your company?
	How do you define trust?
	What influences your feeling of having trust into your employer?
	How is organizational culture influencing trust?
Risk beliefs/privacy concerns:	
Privacy Definition:	What do you understand regarding the term privacy within your workplace?
	Do you think your privacy is protected within your company?
	Are you scared of employee monitoring?
Privacy Risk Belief and Concerns:	Are there processes in your company that are a potential threat to your privacy?
	Do you think it is risky to disclose personal data into software in your organization? And why (not)?
Control:	How would you define control over data?
	Where is the border to loss of control?
Prevention:	How could your employer prevent that you have the feeling of privacy concerns or risk beliefs when disclosing data? (Long term and short term)
Story and Recommendation:	
If you could recommend improvements to your company regarding privacy risk in enterprise social systems, what would it be?	
Can you tell me about a situation where you decided (not) to disclose sensitive information because you perceived it as too risky?	

Table 10: Semi-Structured Interview Guide

The interviews started with a general opening segment by introducing the topic and asking for the team members' roles and responsibilities. The duration of the interviews was approximately 30 minutes and, for generating an open atmosphere, the interviews were scheduled at mutually agreed public locations within the company (e.g., coffee corners). All interviews were recorded and transcribed verbatim for further analysis. Due to technical difficulties, one interview recording was lost. However, additional field notes were taken during the interview. The interview data was complemented with a short follow-up survey which was sent out one week after the interviews to avoid consistency biases. In this questionnaire, the participants' age, gender, job tenure, and further assessed scales to measure both their IT-related knowledge and trust in their teams and the company in general, have been surveyed.

4.5.3. Data Analysis

The analysis of data was carried out using code-based content analysis (e.g., Charki and Josserand 2008; Sarker et al. 2013). NVivo (version 10) was used as software support. It is a tool for qualitative data analysis. The tool offered the ability to organize, categorize, and compare gathered interview data. To reduce the complexity of the whole data set, the tool helped to uncover connections, add insights and in the end, justify the findings. The questionnaire data was assessed and analyzed using SPSS. Initial codes were based on Privacy Calculus literature (e.g., privacy, trust, or demand for control). Further codes emerged during the data collection (e.g., goal incongruences, fear of opportunistic behavior). For instance, the code 'fear of opportunistic behavior' was assigned to the following explanation by an interviewee, asked why he would rather sugarcoat certain information when disclosing it in an ESS: '*Because I'm afraid that this information could be used against me.*' After an extensive reading of all interviews, the codes were iteratively expanded and refined (e.g., persistence of provided Information, value of personal interaction). As an example, the code 'persistence of provided Information' evolved out of the recurring opinion of employees that even though they trusted their employer to date, they did not know if this trust relationship was guaranteed in the future. Not only were additional codes developed during the analysis of the data, but additionally the technological frames perspective on the scenario emerged and therefore helped to develop a structure in coding and analysis. The data was analyzed by locating the topics of the codes identified in the literature. Therefore, Table 11 gives an overview of the thematic codes with a brief description.

The codes were analyzed in relation to the research question. In qualitative research, there are no universally accepted strategies or standards of how to examine the validity or reliability of results, but there are some qualitative methods which can be followed (Venkatesh, Brown, and Bala 2013). Validity, in the qualitative research context, can be defined as the extent to which data sets are credible, trustworthy, and plausible, and consequently can be defended when tested and challenged (Venkatesh et al. 2013). Therefore, to obtain a more comprehensive perspective, the actual coding was conducted by two people. This coding procedure was accompanied by rich comparisons and discussions among the coders to converge in interpretations. The coding results were afterwards integrated to provide an overview of all interviews and relevant passages with

regard to each code. Emerging themes were discussed among the coders to achieve a mutual understanding.

Code	Description
The Employer's Goals of ESS Implementation	Representatives of the employer talk about the actual goals of the implementation of ESS
Beliefs and Interpretations of ESS	Users talk about what they think about ESS and what their personal interpretation is
Users' Goals and Fears	The employee talks about his goals and fears when using ESS
Opportunistic Employer (Privacy Concerns)	The employee is talking about his perception that his employer behaves or might behave opportunistically
Employees' Perception of the Company's Strategy	The employee talks about the perceived goals of his employer when implementing ESS
Trust	The employee talks about what influences his trust into the employer
User Experience and Background	Employees talk about own experience in the past and their interpretations of these experiences
Sensitive Information	Employees talk about information types and how they define sensitivity
Persistence of provided Information	The interviewee talks about the fact that information persistency influences his disclosure behavior
Perceived Benefits	The employee talks about the perceived benefits of using ESS
Anticipated Consequences of Disclosure (Risk Beliefs)	Employees talk about their risk beliefs and anticipated consequences of disclosure
Strategic Information Provision	The interviewee explains that his behavior is some kind of strategic information provision as a behavioral consequence
Demand for Transparency	The employee talks about the demand towards the employer regarding his willingness to disclose information when there is more transparency
Demand for Honesty	The employee talks about the demand towards the employer regarding his willingness to disclose information when the employee would perceive more honesty on behalf of the employer
Demand for Clear Benefit Promises	The employee talks about what he expects from his employer regarding his willingness to disclose information when the employer would show that clear promises are related to disclosure
Demand for Control	The interviewee talks about the importance of information control and related topics, such as anonymity of information and data processing
Environmental Influences	The interviewee explains how environmental factors have an impact on his behavior or perception (e.g., the press or the economic situation)

Table 11: Identified Codes and Description

Considering that there was only little research undertaken regarding sensitive information disclosure in ESS, the aim of this study was to better understand the employee's perceptions and feelings regarding ESS and their employer, rather than to frame a quantitative study that quantified and classified the different quotes of employees. However, the identified codes were mapped to the technological frames perspective in order to build a structure for the analysis (see Table 12).

Technological Frames Perspective	Codes
The Employer's Technological Frame of ESS	The Employer's Goals of ESS Implementation
Employees' Technological Frame of ESS	Beliefs and Interpretations of ESS
	Users' Goals and Fears
	Opportunistic Employer (Privacy Concerns)
ESS Strategy	Employees' Perception of the Company's Strategy
Nature of ESS	Sensitive Information
	Persistency of Provided Information
Usage of ESS	Perceived Benefits
	Anticipated Consequences of Disclosure (Risk Beliefs)
Outcomes from Frame Incongruence	Strategic Information Provision & Resistance
Demand Toward the Employer of the Employee	Demand for Control
	Demand for Honesty
	Demand for Clear Benefit Promises
	Demand for Transparency
Environmental and Cultural Aspects	
Trust	
User Experience and Background	

Table 12: Identified Codes from Literature and Interviews

4.6. Results of Interview Analysis

Going further, the case study results are presented in three sections. The first section provides an overview of the employee's technological frame and the frame of the company, based on the interviews of the HR experts. Furthermore, factors responsible for the employee's beliefs toward their ESS frame will be demonstrated and analyzed. In the end, the resulting behavioral consequences of employees, serving to protect their privacy in ESS, as well as their demands regarding the company's practices will be illustrated.

4.6.1. The Employee's vs. the Employer's Technological Frame of ESS

The company's intentions with ESS implementations were manifold. The main goals were to reduce time-to-productivity by creating communities where employees and new hires could engage with each other, work together on activities, and receive support from experts across the organization. Representatives of the company pointed out that the tools should help employees to feel connected to their teammates and to their employer. Interviewed HR experts also stated that ESS could be very helpful for the organization in skill planning, staffing, employee development processes, and identification of the need for external workforce.

'Let's take an example: Someone is looking for a consultant, with a particular combination of language, culture, and industry knowledge. He can use the tool for that.' –Paul (42, HR Expert)

Furthermore, company representatives had the impression that there was transparent communication regarding security and privacy standards in ESS on behalf of the employer. Nevertheless, they were aware that employees perceived the communication as lacking in clarity.

> *'We are officially anonymous. So there is no possibility to personalize the data. [...] The rule is quite clear, it is documented in the portal, in the operating agreement, and in each quick link... It is completely transparent, but the rules are undermined, which creates an oblique communication.'*
>
> *–Peter (43, HR Expert)*

Despite the company's intentions, employees perceived a lack of transparency with regard to the goals that the organization might follow with the implementation of ESS. In particular, users felt insecure not knowing what the company would eventually do with the data stored within these systems. Trying to reach a conclusion, users arrived at their own interpretations of what these tools were for and how the organization would use data. The significant frame which emerged around the disclosure of information in ESS was that employees were concerned that information which persisted in these systems might be used against them in some kind of way. Although they would not express it explicitly, for most individuals, a natural feeling of suspicion between the company and the individual was always latent. Individuals perceived ESS as possible instruments for the company to reduce employee costs resulting from hidden information and hidden actions. This was an unpleasant thought for many, although a few employees found this kind of relationship natural when working in a company. However, beliefs of conflicting interests between employer and employees were always present: with regard to these systems, employees feared that the organization could be interested in obtaining information to arrive at decisions which would result in unfavorable consequences for employees. Nevertheless, representatives of the employer always pointed out that there was no such intention; rather they were trying to make the life of employees more comfortable with ESS.

Interviewees expressed different ways in which they feared that the company could use ESS data in an opportunistic way. Examples ranged from assessments of work behaviors (i.e., monitoring hidden action) right up to the support of layoff decisions based on evaluations whose skill profiles were not required anymore by the company (i.e., hidden information). However, the main underlying principle was that information disclosure in ESS would create an apparent transparency with regard to an employee's behavior and characteristics that would lead to a shift of power for the employer. As Mark (45, R&D) expressed:

> *'The problem is the asymmetry this creates. Transparency helps only the mighty – not those at the bottom. They make your section transparent, but you don't get to see the whole picture. And with that whole picture, they have a massive advantage. You are supposed to provide information, but you don't get anything in return. That's not fair!'*
>
> *–Mark (45, R&D)*

Interestingly, some employees also internalized their colleagues' well-being, which they did not want to be affected by any data they provided. They anticipated that ESS data might be used to draw conclusions about members of their network such as colleagues or even their managers whom they liked.

> *'Then it doesn't only affect me […] but also my supervisor. Then it's blamed on him that I'm working too much but maybe he doesn't actually want me to, and it's my fault all alone.'*
>
> *–Mimi (27, HR)*

As stated above, some employees thought of suspicion and distrust in their employer as a natural thing. They argued that making the employee's behaviors more transparent would help to establish fairness within the organization and thus had the perspective that such analyses were the right thing to do. *'I think there is no alternative [to analyzing that data]. Some people hide within the company who do not contribute to the company's success.' -Benjamin (27, Consulting).*

While none of the interviewees were really enthusiastic about ESS, some employees had neutral attitudes towards these systems. These employees perceived ESS as potentially helpful if, for example, data would be used to identify the potential for HR training and development. As will be discussed later, these individuals evaluated ESS rather with regard to their effort/benefit ratio. The majority of the participants, however, had skeptical perceptions of ESS, seeing information disclosure in these systems as involving more risks than benefits. In particular, individuals were concerned that information provided in these systems could be used for monitoring and control of their behaviors. For example, users believed that the data could be used to enrich individual's performance assessments or to pigeonhole them. Thereby, two unique aspects with regard to these systems were especially important: data persistence and skepticism regarding the incompleteness of information these systems would produce as support for (staff-related) decisions.

Employee's Technological Frame	**vs.**	**Employer's Technological Frame**
Perception to be vulnerable through sensitive information in ESS because employees assume that the employer might treat disclosed information opportunistically.		Reduce time-to-productivity by creating communities where employees could engage with each other, work together on activities, and receive support from experts across the organization. Help employees to feel connected to their teammates and the employer.

Figure 6: The Employee's vs. the Employer's Technological Frame

Figure 6 gives an overview of the differences between the predominant employees' and the employer's technological frame of ESS implementation. To get a deeper understanding of why

this frame incongruence emerged, the dimensions of the employee's technological frame will be analyzed in the following subsection.

4.6.2. Dimensions Characterizing the Employee's Technological Frame

Why was this opportunistic perspective salient when employees formed their technological frame about ESS? Several reasons for this were encountered, ranging from environmental aspects, perceptions of greed for profit by the company, and trust relationships to differences which related to department characteristics or the employee's job tenure. As in Orlikowski and Gash's (1994) research, three domains could be found that best characterize most of the employee's interpretations made about ESS and the role these systems play within the company and the employee's daily work life. First, the interpretation of the *technology strategy* of the company by the employee, which is directly influenced by the trust relationships in the organization, as well as by the experiences employees have had in the past with their employer and the job tenure. Second, the *nature of the technology*, which is reflected in the fact that disclosed information was often understood as sensitive and persisted in the system. At last the *technology usage* which was mirrored in the perceived benefits and associated consequences of usage as well as employees' privacy risks. Moreover, *environmental factors* such as culture, legal regulations, and the economic situation were found to have an impact on the technological frame of employees.

Influencing Factors on the Technological Frame of Employees

External Factors – Legal Regulations, Culture, and Market Situation

Regarding environmental factors, Roger (35, Consulting) stated that, for example, legal country regulations gave some feeling of safety regarding privacy risks in his home country in Europe since it might be harder for the employer to ignore these regulations. The company might not have the power to impinge a federal privacy law, and therefore, employees might feel safer in countries where laws about privacy are stricter (e.g., Germany or France).

> *'Germany has indeed a relatively extensive data protection law. When you do such things [misusing information], although you stated in a policy that you would not do it, it violates the law.'*
>
> *–Mark (45, R&D)*

Even though there was at least a little trust in country regulations, employees still were skeptical regarding the ruthlessness of their employer and therefore mentioned concerns that their company might disregard the law.

> *'It does not matter what the company says; they do what they want. Even though a company would be truly transparent and say that they do not use data, people would be skeptical and would mistrust. Regulations are always favored towards the employer.'*
>
> *–Roger (35, Consulting)*

However, respondents from the U.S. mentioned that the absence of federal privacy regulations was making employees powerless and because of that forced them to lie or attempt impression management in ESS. They knew that inserted information could be used against them at any point in time.

> *'Even if they are saying that they are anonymizing your data and we do not know who you are. People would still be unsure about that. Americans do not trust in that.'*
>
> *–Sue (45, Consulting)*

All in all, employees were critical in general, and even though there were legal regulations applied in their country employees did not fully trust their employer to fulfil these rules. Nevertheless, interviewees from Europe felt at least a little protected by law, whereas respondents from the U.S. were aware that there was no protection for their privacy at all. As already known from privacy literature, the prevalent culture of a country can play a role in the decision process of whether to disclose sensitive information or not (Krasnova et al. 2012; Smith et al. 1996; Veltri, Krasnova, and Elgarah 2011). Furthermore, it is known that privacy laws also have an impact on the privacy of Internet users (e.g., Johnson-Page and Thatcher 2002; Smith 2001).

Additionally, employees stated that their technological frame might change, based on the economic situation of the employer. A bad economic situation promoted the perception that the employer had to lay off employees and therefore might use information from ESS to select unqualified or bad performing employees.

> *'So in good economic times when everything prospers, everything goes forward, the expectations are high, and everyone likes to share. […] Before, I was working in a medium sized company… and it can happen that a big customer is collapsing and then the company has no more money. […] Then the company has a different value system, how they look at people and their contribution and would of course in doubt access information to decide who should be fired first.'*
>
> *–Tom (47, R&D)*

These environmental factors, difficult to influence by the employer, had a direct impact on the employee's perception of ESS frames and shaped their opinion about the technology strategy of the employer and their need for opportunistic behavior.

Internal Factors – Experience and Mistrust

Beyond these factors that were exogenous to the company's behavior, many actions on the part of the company itself led to the incongruence of technological frames about ESS. The opinion of employees was influenced by the trust relationship to the employer (i.e., senior management) and the employees' past experiences.

As was discovered in prior studies of Privacy Calculus Research in SNS, trust can play an important role in mitigating privacy risks and concerns (e.g., Chen and Sharma 2013; Krasnova

et al. 2012). Similarly, trust played a significant role regarding the employee's uncertainty as to whether the company would use ESS data against them. Being a reciprocal concept, trust was essential in two different ways. On the one hand, employees wanted to be trusted and not to have the feeling that it was necessary to monitor their performance and behavior. On the other hand, trust in their management, or lack of trust thereof, would greatly influence how they interpreted the use of ESS within the company. Trust also materialized as a multilevel construct. Many interviewees stated that they had complete trust in their direct supervisors and that they felt free to discuss even delicate matters with their managers. However, this presence of trust could not be observed across company levels, which was also confirmed by the supplementary questionnaire data (see Figure 7). Employees pointed out how they were affected by decisions made several hierarchy levels above in which trust relationships were absent. For example, Maureen (30, R&D) reported a situation in which 200 of her colleagues were let go by a manager who had no personal relationships with the people affected. Due to this experience, she would not obviously disclose information using a channel to which parties with whom she had no trust relationship had access.

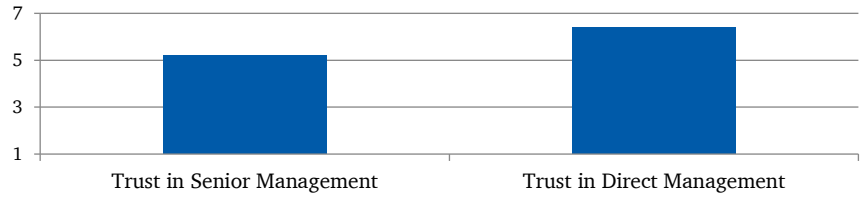


Figure 7: Trust in Senior and Direct Management (7: very high trust – 1: very low trust)

While the employee's trust toward the senior management emerged as a critical factor with regard to information disclosure in ESS, this also seemed to be a very sensitive matter at the same time, being influenced by many little things: *'This implies that a company needs to display a more transparent behavior in so many ways.' -Robbie (30, R&D)*. Overall, this trust dimension was about the question of what seemed to matter more to the senior management: the employee's well-being versus company profit. Whether the company would stand by their employees, even in more difficult times, would make a significant difference with regard to trust.

> *'Let's assume, I'm totally overworked, and then I'm ranked a low performer, this would be a total breach of trust.'*
>
> *–Joanne (55, R&D)*

Although skepticism regarding information disclosure in ESS was more or less present throughout the whole sample, differences across departments and ages could be observed. Compared to R&D workers who were rather skeptical due to their stronger technological understanding and the creative nature of their work (which wasn't normally subject to performance measurement), HR and consulting employees were more faithful toward their employer and viewed ESS more from a rational benefit-effort perspective. Similarly, younger employees were less concerned that the company would use ESS data in an opportunistic way.

The interpretation of this observation was the correlation between age and job tenure, as older employees talked much more about their negative experiences with the company when they were asked about trust and information disclosure. However, even less skeptical employees emphasized that they would still be careful about the data entered into these systems:

> *'I would be careful how I frame it, but I would not worry about giving information. So if someone says: 'How is your manager?', and if I really had a bad manager, I would not mind saying that my manager has some weakness and that he might need coaching. Kind of framing it in a nice way... a constructive way.'*
>
> *–Roger (35, Consulting)*

Technology Strategy

The technology strategy, reflecting the employee's perception of why the employer has implemented ESS, played a significant role in the framing process of employees. The strategy refers to the understanding and interpretation of what drove the decision to adopt ESS and its perceived related value for the employer.

Given that employees perceived that management had repeatedly laid off some of its workforce despite substantial profit gains, the employee's perceptions were that information provided within ESS could be used to identify low-performing workers or employees with skill profiles which could be disposed of more easily. Employees believed that extensive optimization of input-output had a higher prioritization by management than their well-being, and thus ESS might be used to reduce costs (i.e., identify ineffective or dispensable workers). In this regard, individuals assumed that their company could search for hidden information or might do so in the future, due to the persistence of data. The company further contributed to individuals' perceptions, making them believe that the management explicitly ranked employees by their performance. For instance, a while ago, a new tool was implemented within the company, used to evaluate the performance of employees based on the subjective opinion of the people's manager. Thereby, employees were categorized into performance groups such as 'high potentials' as well as 'low performers'.

> *'Even when they introduced the terms 'low' and 'high performer' it seemed to me as something negative. […] This was already a concrete breach of trust for me.'*
>
> *–Joanne (55, R&D)*

Generally, the communication of the goal of a software tool introduction played a significant role. The more untransparently an introduction and rollout happened the more people perceived a risk behind such a tool. Peter (43, HR Expert) stated that he thought that transparency and clear rules were the two things that would help employees not to perceive a system as a threat.

> *'[…] what would help? First, clear rules and second complete transparency of these rules. I think this would help and everyone could decide on his own if he wants to participate or not.'*
>
> *–Peter (43, HR Expert)*

This impression was also supported by the employees themselves, as Benjamin (27, Consulting) and Joanne (55, Developer) stated that they would offer information when they knew what would happen with their information and agreed with the usage.

> *'When I know what is happening to my provided information I would participate. For example, when participating in the employee survey I know that the data is provided to the senior management and they make a plan with counter measures.'*
>
> *–Benjamin (27, Consulting)*

In sum, the employee's perception of the employer's strategy of introducing ESS seemed for many employees as implementation of a control structure, even when they had the feeling that work was done properly. Even though employee surveys are not understood as an ESS, employees mentioned their concern when answering the questions. In general, where honest feedback might be valuable for the company, employees rather tended to answer in a strategic way, as they presumed a strategy and possible hidden agenda behind such a questionnaire.

> *'I think people generally are not a 100% honest on their survey, because even if they say that it is anonymous and they won't know who has answered, I think that some will come back to us when people are answering honestly.'*
>
> *–Sue (45, Consulting)*

Nature of Technology

The nature of technology generally refers to the employee's understanding of the abilities and functionality of ESS. In this study, two aspects of the nature of ESS were found – first, the employee's understanding of the sensitive information types inserted into ESS, and the fact that this delicate information could be persisted for a very long time.

Employees perceived several information types requested by ESS as sensitive. They were also evaluated differently by different people. Sensitive information types ranged from personal health information over the salary to personal opinions or political attitude. For example, Maureen (30, R&D), as well as George (27, R&D) perceived their personal health status and information as sensitive and thought that this was nothing they would share with their employer. On the other hand, Benjamin (27, Consulting), who was generally more open, stated that he would have no problem publishing his health information if it would be helpful for his manager to staff people on projects. He would, rather, hesitate to reveal his salary to others in ESS. All kinds of information could be included in several ESS of the company and, even though there were different opinions about the types of information which should be rated as sensitive, all employees defined sensitivity of information as the fact that every information attribute was assumed as sensitive, which had a negative impact on them: *'[..] In case of doubt, everything that can be used against me.' -Gordon (45, R&D)*. For instance, Tom mentioned:

> *'Sensitive Information is everything, […] that offers another person the possibility to build a position of power against me which I cannot control.'*
>
> *–Tom (47, R&D)*

Furthermore, the fact that employees wanted to decide with whom they wanted to share their information was an indicator of sensitivity. This goes along with the general definition of 'Information Privacy' by Westin (1967), who claims that information privacy is an individual's demand to determine for him- or herself when, how, and to what extent information is communicated to others. Hence, related to sensitive information asked by the company through ESS, employees demanded information privacy. As, for instance, Benjamin (27, Consulting) stated *'The term 'sensitive' in general means for me that I want to decide on my own who has access to my information.'*

Moreover, persistence of the information entered into these systems was seen as problematic. Once personal information or opinions were disclosed, there might be no way to take it back. The information would be stored on some server of the company and could, from then on, be used as evidence in one way or another by the organization. Even when individuals fully trusted the company's current management, they expressed uncertainty about future developments and the possibility that company related changes (i.e., new management) could lead to the unwanted use of persistent data in future contexts:

> *'What prevents me [from sharing information] to a great extent is that, once data are gathered, personal data are made persistent, they're there. And if things change, if board changes, if strategy changes, you can't tell for sure what they will use the data for.'*
>
> *–Tom (47, R&D)*

Information is understood as persisted when it is available in the same form as the original information after a person has finished disclosure (Bregman and Haythornthwaite 2003; Donath, Karahalios, and Viegas 1999). Employees, therefore, preferred communication channels which had no such documentation functionality, like personal conversations or phone calls. Related to this issue, employees regarded the 'out-of-context nature' of information stored within ESS as problematic. For example, individuals stated that they had no problem at all expressing their opinions or constructive criticism toward their supervisors. However, in a context of big data and machine learning, they would rather not disclose information in these systems which could be falsely interpreted when taken out of context. Users feared that wrong assumptions would be made based on algorithmic data analysis, delivering only incomplete pictures of the truth.

> *'Systems tend to draw conclusions regarding your personality based on your past behavior. This doesn't match my personality and I want the freedom to be perceived in different ways. I think it's too narrow.'*
>
> *–Joanne (55, R&D)*

It can be concluded that employees perceived a potential of threat regarding the nature of ESS, in particular, because of the sensitivity of information that was asked for and moreover, because of the fact that sensitive information was persisted in software. Employees hesitated to disclose all information into ESS that seemed for them to shift control towards the employer and offer him the opportunity to wield power over employees.

Technology Usage

The third domain in focus of the employee's technological frame of ESS is their interpretation of how ESS could be used in day-to-day business and how they could generate benefit from it.

As also found out from Privacy Calculus Research in SNS, benefits can mitigate concerns and risks and lead people to disclose more sensitive information than they actually wanted (e.g., Chen and Sharma 2013; Hollenbaugh and Ferris 2014; Krasnova et al. 2010). This also holds true for the present scenario of ESS. When employees perceived a benefit from disclosure they were more willing to contribute to blogs or social networks of their company than without any perceived benefit. As, for example, George (27, R&D) stated about the insertion of information into a skill database: *'It is somehow too much effort, and I do not use things that are taking too much effort and where I do not see the direct benefit.'* Even though there was much skepticism toward ESS usage and the resulting benefit from disclosing information, few employees said that the value of using ESS would make them disclose sensitive information: *'I think that with the provided information you can achieve positive effects [for the company], and this would, in turn, have a value and benefit to me.' –Nic (25, R&D).* So, if employees really perceived a benefit, they were willing even to reveal information they would classify as sensitive and despite that there could have been a potential for perceived loss of information privacy:

> *'The self-representation factor would definitely motivate me [to disclose]. People, who I want to impress could become attentive to me. On the downside, it is a fine line. Other people, I don't want to become aware of me, could also become attentive to me.'*
>
> *–Mark (45, R&D)*

This process of deciding whether to disclose information or not, by weighing risks and benefits is very well known from privacy research and can be found in several studies of privacy research in SNS (e.g., Dinev and Hart 2006; Krasnova et al. 2012; Sipior, Ward, and Connolly 2013).

4.6.3. Behavioral Consequences and Demands toward the Employer

In addition to conclusions about the employee's technological frame of ESS, insights about the behavioral consequences and the demands of the employees toward their employer became obvious during the interviews. As they were concerned about power shifting towards the company, employees perceived active privacy protection as a countermeasure which was at least partly under their control. As ESS was seen to serve the company as a control structure, reducing the demand for information and creating transparency, users would consciously try to monitor the information they disclosed, trying to avoid negative impressions or to present themselves favorably. All in all, the protection of privacy was seen as a protection from harmful actions on the part of the organization. On the other hand, employees believed that, from the organization's point of view, the employee's privacy would be a negative thing, impairing control over the employee.

Several behavioral consequences resulted from the employee's beliefs which all had immediate implications for the quality of information stored within ESS: providing false information or no

information at all as well as exaggerated self-presentation. Voluntary ESS use would thereby sometimes tend to result in no information disclosure at all: Gordon (45, R&D): *'The best data protection is not providing any.'* Another, less drastic, but still not preferably reaction was lying and exaggerating. As, for example, Joanne (55, R&D) would never insert the truth about her (not existing) skills into some system but rather would try to conduct impression management, to prevent negative consequences for herself: *'I would not insert that my English is not that good as it should be. I would try to insert that I am good in all skills that are expected from me.*' When asking about the consequences of forcing employees to use ESS, individuals furthermore stated that this could lead to a strategic provision of self-presenting information. *'Although you don't lie, you'll tend to disclose information which will have some kind of positive effect.' -Mimi (27, HR).* Moreover, one employee even stated that he would try to harm his employer when he would try to force him to use an ESS: *'And when they annoy me too much, I would think of how I can cause the greatest damage to the company.' –Gordon (45, R&D)*

When asking the employees what their employer could do to further improve acceptance of ESS and thus realize the benefits of ESS, four aspects were mentioned in particular. First and foremost, employees strongly demanded transparent communication regarding what happened with the data they provide. Given the technological frames perspective described above, ESS were seen as a black-box in which employees could enter data that would eventually inform the management based on undisclosed algorithms and lead to unfavored decisions. Even Benjamin (27, Consulting), who was generally supportive of ESS data analysis, emphasized his desire for transparency:

> *'I have no problem in providing information, but I want to know what's done with it. […] It's better to disclose a KPI [for reducing staff] instead of hiding it.'*

As a second point of emphasis, employees demanded control over their data to actively manage the impression that was built upon information inserted into ESS. This included being able to view available data, anonymize certain information, and to delete it at a later point in time.

> *'[…] situations change, managements change, contexts change and, all of a sudden, data appears in a whole different light as opposed to when I provided it trustfully. I want to be able to delete it.'*
>
> *–Joanne (55, R&D)*

Moreover, employees requested honesty on behalf of the senior management so they could have the feeling that their company is of integrity and wants to build a trust culture. As for example, Mark (45, R&D) said that his company could show him that they want to build a trust culture, by *'living up to their promises'* and that they should *'give employees a leap of faith so that they can make mistakes without fearing subsequent existential consequences*.' Furthermore, the demand for honesty also confirmed the need for a more culture of integrity and mutual trust. Employees argued that honesty would make them trust much more in their company. As in the past, they have experienced that the senior management tried to embellish their decisions and behavior they demanded their company to be straightforward, although this might be an admission of

weakness. On the contrary, in the eyes of employees, this would be rather a sign of strength and trust. *'In such a position [meant is senior management] it is a must to communicate own mistakes because exactly that builds trust.' -Benjamin (Consulting, 27).*

Finally, it seemed that employees demanded a real and definite benefit promise when disclosing sensitive information as quid pro quo. *'The key is a central and real benefit promise, an immediate benefit. I give so that you give.' -Christopher (R&D, 27).* Obviously, employees perceived that many promises was not kept when they disclosed information in the past. In particular, concerning the present employee survey, employees argued that they do not recognize any benefit or even worse, perceived detriments from disclosure. This provoked frustration and information refusal. Hence, real benefits would motivate the employee to participate in an honest way in ESS.

All in all, employees' reactions were strategic data provisioning. This was reflected in favorable coping, data refusal or impression management. Furthermore, employees demanded from their employer to develop a culture where they had the feeling to be taken serious by providing all necessary information in a transparent way. It was also demanded, that the senior management should communicate honestly about everything, even though it is something unpleasant, by handing over control of sensitive information stored in ESS to the employee and in the end by keeping promises and offering immediate rewards from disclosure. As one employee mentioned:

> *'You [as an employer] have to proof that you take feedback from your employees very constructively. The company has to develop a new HR culture that gives the employees the feeling that the company is in his favor.'*
>
> *–Christian (R&D, 40)*

4.7. Summary

The results of the analysis show that employees reacted with strategic information provisioning into ESS and other enterprise information systems, such as the digital employee survey, since they perceived privacy concerns in the form of opportunistic behavior on behalf of the employer. This was reflected in favorable coping, impression management, resistance, or information refusal on behalf of employees and hence resulted in false information provision or no information provision at all.

As Orlikowski and Gash (1994) already emphasized in their vital work for technological frames, if there is an incongruence in frames it is likely that problems exist in implementation and usage of technology. In line with their argumentation, the results of the analysis show that the disclosure behavior of employees is also based on the incongruence of the frame of the employee and the employer. In particular, between the perceptions of employees what the goal of the company was to introduce ESS and the actual implementation goal of the organization. The employers' primary objective with the introduction of ESS was to help employees to reduce their time-to-productivity by building communities, connecting people or the employer, and to support skill planning, staffing, and employee development processes. Nevertheless, most of

these aspects and intended benefits for employees and the employer were not recognized by the workforce. The majority of employees showed skepticism towards ESS, seeing more risks than benefits when disclosing sensitive information into those systems. Especially, people were concerned that the employer could use provided information for control and monitoring purposes. Accordingly, the employee's technological frame of ESS can be described as the employee's perception that he is vulnerable when disclosing information into ESS because they assume opportunistic actions with provided information of the employer as the highest risk factor.

The employee's technological frame is based on several observable aspects that formed the impressions and beliefs about ESS. These aspects can be described based on three dimensions of the technological frame as well as environmental aspects that are further influencing the employee's interpretations. In particular, their perception was shaped by the prevailing perceived ESS strategy of the company to monitor and dispose people with the help of ESS. This perception was based on the prevailing opinion that there is a lack of mutual trust and related negative experiences with the company. Apart from that, employees had their specific interpretation about the usage of the technology. Hence, the perceived related negative consequences of disclosure and the lack of obvious benefits were even increasing the suspicion and wariness of employees. Additionally, the nature of ESS also influenced the impression of the workforce that ESS might be used as an opportunistic instrument. The sensitivity of requested information and the technical property that this information was persisted in databases made employees vigilant and cautious. In the end, external factors, such as cultural aspects, legal regulations, and the economic condition were influencing the employee's beliefs about ESS and the perceived strategy of the company (see Figure 8 for an overview of the results).

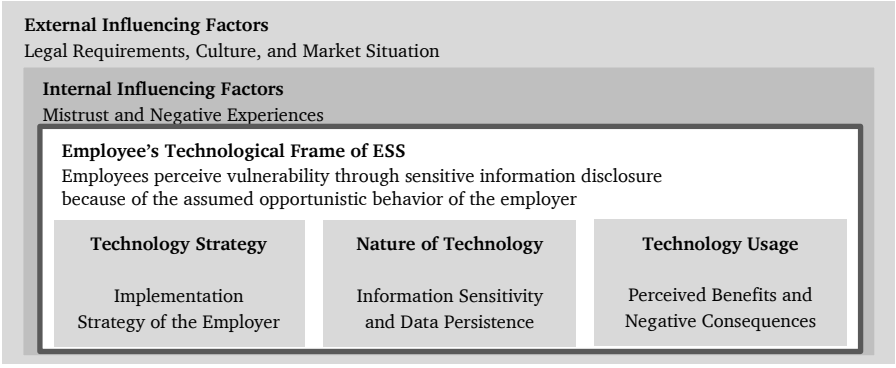


Figure 8: Overview of the Employee's Technological Frame of ESS

To overcome the frame incongruence on behalf of the employee, they demanded a mixture of real observable benefits, control over their provided information, transparency about employee actions and intentions, and an honest culture of integrity where everyone could speak up and was taken seriously. First and foremost, these demands were mainly based on experiences they made in the past regarding information disclosure and very often related to the prevailing culture

in the company. In many situations, employees perceived a relatively high degree of mistrust and dishonesty on behalf of the senior management towards the workforce, which in turn lead to doubts regarding the company's intentions regarding ESS implementation. Over and above, employees demanded more control over their information goods and profound insights regarding information processing and further data analysis. Since the general perception about sensitive information was that it is some kind of personal asset which belongs to oneself, this demand for controlling the flow of information and further understanding about processing goes in line with findings from information privacy literature and seems quite natural. Information privacy is the claim of people to decide for themselves when, how, and to what extent they want to share information with other people (Westin 1967). Hence, the demand for sensitive information control and transparency about information processing of employees seemed like a more or less basic need and should be considered by any company when introducing ESS.

When having a more precise view on the dimensions of the employee's ESS frame several aspects from already existing Privacy Calculus Theory can be found. Those are aspects and dynamics which are also present when people decide to disclose information into private SNS. For example, cost-benefit dynamics can be found during the decision process whether to use an ESS or not. Employees decide for information disclosure when they perceive a benefit that is outweighing their concerns and risk beliefs. Nevertheless, those observable factors and dynamics are interestingly of a different nature and enriched with further aspects, stemming from the employer-employee specific context. For instance, the study disclosed that qualitative and sustainable usage of ESS might only happen when employees feel protected in their business environment. Companies have to consider their prevailing culture. Employees demand a high degree of mutual trust and honesty on behalf of the senior management. If this precondition is not sufficiently met, employees will probably perceive much higher risk and privacy concerns when thinking of sensitive information disclosure in ESS.

4.8. Discussion of Intermediate Results

The aim of this section was to provide rich insights regarding the employee's beliefs about ESS, influencing factors, as well as behavioral consequences with regard to the disclosure of quality information in ESS. The results showed how employees perceived such systems against the backdrop of the ESS frame of the employee and its incongruence to the one of the employer. Therefore, a qualitative study was conducted with 22 employees and company representatives of a globally acting company. While a few employees had congruent frames with their employer, a significant share of participants had rather negative and different attitudes toward ESS, interpreting them as instruments for monitoring and control which would support employer opportunism. Although exogenous factors like regulatory structures or the company's economic stability were mentioned as influencing factors, central for the employee's attitudes were factors stemming from the employee's relationship to the employer and from Privacy Calculus Research. For instance, their experiences with the company, their trust in the company's management activities, the perceived negative consequences of disclosure and the lack of perceived benefits

were reasons for the incongruence and concerns. Going further, the study's contributions to theory and practice as well as its limitations are going to be discussed.

4.8.1. Contributions to Theory and Practice

First, the study contributes to research on privacy and sensitive information disclosure. Since previous studies in this regard have focused their efforts on public SNS, there is a need for studies on the employee's beliefs and behavior with regard to ESS. As opposed to public SNS, users of ESS strongly depend on the network provider, i.e., their employer. For the research of this section an interpretive approach was applied to offer deep insights regarding the formation of the employee's beliefs and behaviors toward ESS in the light of technological framing. It was found that these beliefs are strongly influenced by the relationship quality between users and the company.

Along these lines, it was found that Technological Frames Theory serves as a fresh and valuable perspective on ESS acceptance and the quality of an individual's ESS use in particular. The theory has mainly been applied in enterprise contexts where organizational change regarding IT was in focus (e.g., Davidson 2006; Leonardi 2011). However, as shown in this research it applies as well in EIS research contexts in which self-disclosure is key for EIS success but at the same time can alter the balance of power between the employer and the employee, such as ESS. The case study has shown that ESS can be perceived as a means for monitoring and control, consequently shifting power toward the employer. Employees' concerns about opportunistic behavior on behalf of the organization are thus likely to adjust their information sharing behavior in their favor which may be detrimental to ESS success. These considerations should become more and more relevant for future EIS studies, given the current increase in produced information (e.g., mobile data, social information), HR analytic tools, and the data value in general (e.g., Chui et al. 2012).

With regard to critical influencing factors which contribute to (in)effective ESS use, this study shows that the degree of which users are concerned that their organization would act in opportunistic ways plays a central role for the technological framing of employees and related self-disclosure in ESS. If ESS are introduced in a context in which employees perceive their employer to act opportunistically, chances increase that users interpret ESS as tools for monitoring and control. Furthermore, risk-averse employees are influenced by their uncertainty about the future. Even when trusting the current management, the possibility for opportunistic behaviors in a future context influences the employee's behaviors in the present due to the persistency of data. Companies who are deciding to implement an ESS should be aware of the current climate within the organization and the employee's beliefs regarding perceived organizational opportunism and therefore adapt their technology implementation strategy.

The study further illustrates that trust toward the upper levels of management seemed to affect the employee's attitudes toward ESS greatly. This presents an interesting perspective as ESS are often aimed at fostering information sharing across hierarchy levels and thus should break up

strict company structures. As outlined above, this goal might be difficult to achieve if trust relationships are absent across hierarchy levels.

Interpreting ESS as a tool for monitoring and control has immediate consequences for the quality and quantity of information provided in these systems. Employees who fear that information might be used against them would tend to provide less or no information at all or might overly engage in favored exaggeration if they believe that their performance evaluations depend on such data. Even destructive behavior could be a result of incongruent frames. The resulting data might then misrepresent the actual issues and challenges within a company which would imply that further time and effort spent in ESS would be ineffective. Thus, although analyzing ESS data might seem like an advantage of ESS at first, this study shows that companies should be very careful tapping this potential. In any case, it seems inevitable for a company to first promote company-wide trust-relationships in which transparency and honesty are perceived reciprocally. Otherwise, analyzing ESS data and, on top of that, linking results to performance-related salaries could lead to an unhealthy competition among employees and an abuse of these systems.

Furthermore, as these interpretations of ESS frames by employees are not necessarily aligned with the actual intention of companies, employers should engage in frame alignment. As Orlikowski and Gash (1994) emphasize when incongruence exists, the probability that problems during implementation and usage arise is very likely. To prevent misaligned beliefs, unanticipated consequences and contradictory actions of all user groups, an initial valuation of the frames should be done. The significance of initial identification of incongruence in frames of ESS and anticipations regarding its introduction should take place as early as possible. It is of essential importance to seek for alignment and mutual understanding among the groups in the company. Therefore, it is important to involve all stakeholder groups which will be affected or are affecting the implementation of the ESS in question. For instance, highly influential managers, and the members of different occupational subcultures whose ways of working or modes of thinking are to be altered should be involved in the clarification process. First, the assumed nature of the ESS to be implemented should be made transparent to all involved stakeholders; second expectations and goals of the company concerning the implementation should be communicated honestly, and third the employee's benefits from using the ESS sustainably should be addressed in detail to mitigate their risk beliefs and increase their motivation. However, it should be emphasized that all these measures will not take any effect if employees do not perceive a mutual trust culture, where honesty and transparency are valued and desired.

It can be concluded that factors stemming from the employer-employee relationship, as well as technological factors are influencing an employee's decision to disclose decisively. This unique characteristic should be considered for further research on ESS and the perceived privacy of employees in the organizational context.

4.8.2. Limitations and Further Research

The results underlie several limitations, indicating interesting ways for further research. First, the insights are based on a single case study conducted in only one company. Although this case was chosen deliberately due to its interesting context, it would be valuable to study cross-company differences in ESS acceptance in the future. Thereby, the findings of this research provide valuable insights regarding the factors which influence ESS success. Future empirical research could use the results as a starting point, conducting qualitative or quantitative studies across contexts and cultures. For instance, future studies could investigate whether employees with different valuations for liberties within a company also vary in their perceptions of ESS. Furthermore, analyzing how differences in the modes of performance measurement between units (e.g., sales vs. R&D) might affect ESS attitudes could yield valuable insights.

Second, the results suggest that inter-temporal effects (e.g., company history, personal experiences, and expectations about the future) affect the employee's present attitudes and behaviors toward ESS. Comparing the relative impact of past events and uncertainty about the future in relation to the current situation should present a highly interesting endeavor. Thereby, the use of longitudinal research methods could provide a promising approach.

Third, the findings illustrate that the employee's interpretation of ESS and hence his information disclosure behavior seems strongly dependent on the employee's experience on how trustworthy, fair and truthful his employer intends to act. Incorporating theories from social science, examining the employee's experiences and resulting expectations toward the employer's trust behavior, might be a very interesting attempt to clarify and further understand these dynamics. For instance, psychological or social contract theories might serve as a good starting point for this perspective.

Fourth, both the employer's and the employee's actions are influenced by uncertainty about the future. As everyday life shows, the more uncertain a company's future, the more important the reduction of costs might become (e.g., laying off ineffective employees). For employees, on the other hand, fears of being evaluated as ineffective should increase their concerns about their privacy. This may present a vicious cycle with regard to ESS use, which could be hard to overcome. Future studies could investigate on possible leverages for companies and users to break up such dynamics.

Fifth, not only ESS are affected by the employee's negative technological frame and concerns about privacy. It seems that there are several other EIS that have the potential for employees to be a threat. Future research could focus on this fact and elaborate on a potential new class of enterprise information systems, comprising specific characteristics that lead to a high perception to favor opportunistic behavior on behalf of the employer. This class could help to better understand and classify EIS with regard to SID.

Moreover, the results yield numerous possibilities for future research concerning technological frames. For instance, previous research on this issue has suggested that environmental and cultural aspects have to be considered when evaluating technological frames of user groups (Davidson 2006). Even though this study gives a glimpse of how these environmental factors might look like, further research should be conducted that studies the evolution of technological frames on ESS with regard to the environment and the cultural setting of companies. Moreover, the application of Technological Frames Theory in IS has mainly focused on using qualitative methods to elicit frames, understand their incongruence, and in the end engage in alignment. In this regard, research could be expanded to think in a more quantifiable direction and extend investigation with quantitative data, to increase the validity of ESS frames. Another possible next step could be the extension of research on ESS in the context of technological frames into a more holistic direction. The research of this section has mainly focused on the perspective of the employee and highlighted challenges and demands of the workforce toward employers. For an even more holistic approach and a better understanding of the incongruence of frames in ESS, it would make sense to emphasize on both sides of the medal and additionally examine the frame of the employer and his demands toward his workers in more detail.

In closing, it does appear that the success of ESS is highly dependent on the employee's willingness to disclose sensitive information. Hence, companies have to invest time and effort in clarifying their expectations and motivations of implementation, as well as building a trustworthy and honest culture, where employees feel safe to speak up in the present and the future. This is a tough way forward which has to be considered in the long run since culture and trust cannot be built easily but destroyed in minutes. Therefore, it is important to involve all groups of a company, starting from the senior management to the smallest employee, into the implementation process. For theory this research showed that there are several similar aspects influencing an employee's privacy risk beliefs and therefore his willingness to disclose sensitive information in private settings as well as in the company setting (e.g., demand for control of disclosed information or degree of information sensitivity). Nevertheless, there seem to be even more relevant dynamics and influencing factors stemming from the relationship between an employee and his employer, that are unique to this scenario (e.g., experiences in the past, mutual trust culture, or assumed implementation strategy).

5. The Employee's Perceived Information-Based Vulnerability – A Research Model

5.1. Introduction

Many of today's enterprise information systems (EIS) require employees to make correct information about their skills, activities, or opinions available to their organization. In this thesis, we argue that the success of these systems depends strongly on the relationship quality between the employees and their employers. Based on the Privacy Calculus and Psychological Contract Theory, a conceptual framework is developed and empirically tested, that features a user's perceived information-based vulnerability (PIBV) of a system: a construct that reflects a user's perception that information entered into a system could be used in an opportunistic manner by the employer. The framework suggests that employees who fear that a system serves as a potential data source to inform their employer about abilities and fulfillment of duties, will reduce the quality of their usage. This section helps to understand the peculiarities of revealing enterprise information systems (REIS) which depend on employees' disclosure of skills, activities, or opinions to their employer. [6]

Organizations are investing considerable amounts of time and money to implement information systems such as enterprise social networks, knowledge management systems, or mobile apps, to enhance employee performance and to increase organizational success (e.g., Koch et al. 2012; Treem and Leonardi 2013). While straightforward workflows guide the usage of many information systems, the actual value of certain others depends on the readiness of their users to supply information about themselves and their activities (Eisenberg and Witten 1987; Gibbs, Rozaidi, and Eisenberg 2013). Such systems depend on employees who share their professional skills (Koch, Gonzalez, and Leidner 2012; Koch, Leidner, and Gonzalez 2013; Treem and Leonardi 2013), locations (Junglas and Watson 2008), status (DiMicco et al. 2008; Koch et al. 2013), activities, thoughts, or opinions (Denyer, Parry, and Flowers 2011; Hurbean and Fotache 2013; Koch et al. 2013). Examples of current systems which require employees to reveal such information are enterprise social systems (e.g., internal social networks, blogs, and wikis), employee feedback systems, or location-based mobile enterprise apps (Berghaus and Back 2014; Gibbs et al. 2013; Hurbean and Fotache 2013; Mokbel, Chow, and Aref 2007). Based on the results of the previous qualitative study on enterprise social systems (ESS) and sensitive information disclosure (SID) of employees, it could be shown that it is important for companies to understand what prevents and motivates employees to disclose honest information into these systems about themselves. Otherwise, the investment might have failed its purpose. Furthermore, it could be revealed that reasons for such behavior might not only stem from the system and its characteristics itself, but from the relationship an employee perceives with its company. Employees who, for example, perceive that disclosed information might be used to harm them will not use the system or even might react with a negative attitude. Therefore, the

[6] This section is based on the publication: Träutlein Sarah, Gerlach Jin P. "Perceived Information-Based Vulnerability of Enterprise Information Systems: Concept, Antecedents, and Outcomes." in *Proceedings of the 36th International Conference on Information Systems*. 2015.

present thesis goes one step further and suggests a new perspective on enterprise information systems. The systems have in common that their value for the employer depends on users' readiness to provide truthful information about themselves (including ESS).

5.1.1. Motivation

What kind of perspective is proposed in this research and why is such a perspective valuable? For systems of this nature, it is more important to investigate the quality of usage when assessing their success than it is for other classes of IS, as it depends on users who provide both sensitive and correct information about themselves and their work. Employees might have different expectations, assumptions, or knowledge about any core feature of a system then their employer and might, in turn, assume opportunistic behavior. Hence, they might react with information refusal or strategic information provision in these systems. This perceptual incongruence of software systems is described in software science as incongruence of technological frames of stakeholders (Orlikowski and Gash 1994). For instance, incongruence of a frame is present when line managers assume that a software transforms their organization in how they are doing business, but on the other hand, users believe that the system is implemented to simply control their work and behavior. Moreover, the success of an ESS is questionable if employees insert what they think will present them favorably in front of their managers and companies and therefore use these systems for impression management (Birnholtz, Dixon, and Hancock 2012; Gibbs et al. 2013) or to protect themselves from assumed opportunism of the employer. For example, consider an HR 360-degree feedback system that will not fulfill its purpose if users do not share their honest and open opinion how their managers are running the organization but rather fear that criticism might be traced back to them. At the same time, high-quality usage of these systems should be hard to enforce and control as the sincerity and correctness of user input cannot be determined easily by objective criteria. In sum, the success of these systems strongly depends on the quality of information entered by employees about themselves. For the ease of argumentation throughout this thesis, the label 'Revealing Enterprise Information Systems' (REIS) will be used – suggesting that information within these mentioned EIS is more or less revealing for the user who provides it.

In this thesis, a closer look is taken at REIS and their unique characteristics, which determine their success in a particular way. As REIS depend on users revealing information about themselves with their employer, the quality of REIS usage should be closely related to the relationship quality between employees and their organizations. To better understand the nature of this class of enterprise information systems, we refer to the technological frames perspective. The theory has been used to learn about the cognitive structures that shape a technology user's perspective on IT, its usage intention, as well as assumed consequences resulting from IT adoption (Orlikowski and Gash 1994). As the previous section already showed, the perception of an employee's experience and trust relationship with the employer have an impact on the employee's technological framing and in turn on their disclosure behavior. Revealing information within REIS means that a user actively decides to trust his employer – by disclosing his or her activities, skills, or opinions – that his information is not used against him and

opportunistic motives do not drive the implementation strategy of the company. Therefore, the quality of the employee–employer relationship, which is the subject of Psychological Contract Theory (e.g., Morrison and Robinson 1997; Rousseau 1989; Rousseau and McLean Parks 1993) should determine an employee's anticipation of opportunistic behavior and thus the quality of REIS usage. The theory describes an employee's subjective expectation of how his employer should behave and act toward him and his environment (Morrison and Robinson 1997).

In order to conceptualize this rationale, a new construct is proposed – the perceived information-based vulnerability (PIBV) of REIS – which captures a user's perceptions that information entered into a system can be used in an opportunistic manner by the employer. As PIBV displays a perceived system characteristic, organizations can evaluate REIS in order to get a feel for the system's future success. Over the course of this research, antecedents and outcomes of PIBV are proposed and empirically tested. Furthermore, a validated measure of this newly developed construct is supplied.

5.1.2. Derivation of Research Question

According to the previous considerations on the challenges coming along with REIS implementation and lack of investigation, it can be argued that IS research on sensitive information disclosure should be conducted to complement previous findings and support successful implementation. Therefore, this subsection deals with the following research questions:

1. *How is the perceived information-based vulnerability of employees influenced by the employer-employee relationship and specific characteristics of revealing enterprise information systems?*

2. *How are perceived information-based vulnerability of employees and the perceived benefits from disclosure affecting the employees' usage of revealing enterprise information systems?*

To answer these questions, a research model will be developed, tested and evaluated. An exemplary REIS is going to be examined for its PIBV, the influencing variables and the resulting outcomes. The results contribute to theory as they extend research on sensitive information disclosure in IS toward organizational settings. It emphasizes the importance of the employer-employee relationship, as well as technology characteristics in this regard. Furthermore, resistance as alternative outcome to information disclosure will be presented and discussed. In addition, the results contribute to practice as the insights can guide companies to successfully implement REIS and prevent failures in this regard.

Going further, a broad overview of the Privacy Calculus Theory and Technological Frames Theory is given. The Psychological Contract Theory is presented in detail. All three theories serve as theoretical foundation for the research. Afterwards, a more detailed elaboration on the nature and definition of REIS is presented. In the subsequent chapter, the construct of PIBV is defined and described in detail. The developed research model was tested and evaluated by a survey study. Results of this study will be presented in the following. Afterwards, the results will be analyzed and discussed. In the end, this subsection concludes with a summary of the contributions to research and practice.

5.2. The Nature of Revealing Enterprise Information Systems (REIS)

The framework may, in particular, have relevance for the implementation, development, and administration of information systems that have the goal to reveal personal and sensitive information from employees. Even though all EIS can have the characteristic of PIBV, it can be assumed that there are specific features of EIS that might increase the probability that PIBV is high. Therefore, this subsection explains the dominant characteristics of so-called REIS:

1. The employee actively discloses information into the system
2. Disclosed information tempts misuse and opportunism of the employer
3. System success depends on honest information provision by the employee

The label REIS thus subsumes EIS which require their users to make revealing information about themselves available to the organization for the system to be successful. Information items are considered as revealing if they help drawing conclusions about an employee that might be relevant to his or her employer, such as his or her personal life, expertise, abilities, well-being, attitude, activities, or location during work time. According to this, one characteristic of REIS is that information inserted by the employee can be perceived as a potential threat since the employer might use it for opportunistic purposes. Taking a look at the employee's daily work, several applications can fall under this category. For example, enterprise social networking platforms, employee mood measurement tools, wikis, (micro-)blogs, and other knowledge sharing systems or location-based mobile services make employees to revealing potential sensitive information (e.g., their activities or opinions). All of these enterprise information systems are more or less dependent on the willingness of employees to provide correct and honest information (e.g., Denyer et al. 2011; Koch et al. 2013), whereby the willingness of employees to provide correct information does not imply that the usage of REIS has to be voluntary. It rather indicates that employees actively have to decide whether to disclose accurate and honest information or not. If employees are uncertain about the employers' intentions, due to suspicions regarding the purpose of the application of the enterprise system, it is hard to verify if the information provided is actually honest and accurate. On the other hand, a software solution that only requires sales orders or bills from employees are not part of this class of enterprise solutions, as characteristics are not fulfilled. Employees can actively decide to disclose information but the type of information does not lead to the fear of opportunistic behavior of the employer.

REIS can offer many benefits to employees and the organization as a whole as they generate visibility and transparency regarding the employee's knowledge, activities, preferences, and social network connections (Treem and Leonardi 2013). For instance, companies can use 'expert finders' or 'skill databases' in which their employees are requested to provide their competencies and experiences to enable other employees access to expert knowledge (Mattox, Maybury, and Morey 1999; Yimam-Seid and Kobsa 2003). In a similar vein, wikis offer a simple way for employees to publish information and make work-related knowledge and activities visible to co-workers (Grudin 2006). Moreover, REIS can enable employees and employers to archive

information and therefore facilitate an employee's daily work. For instance, conversations can be persisted by engaging in social media, such as recording discussions with video-conferencing tools, instant messaging, or email. Persistence supports the development of a mutual understanding in communicative settings, document outcomes of conversations, and to give others time to fully understand conversations (Treem and Leonardi 2013). Further and foremost HR trends show that REIS will become more and more important in the HR landscape, as HR analytics gains ground in organizations and demands for employee information (Romrée et al. 2016). Companies expect a big additional value from HR analytics and immensely invest in tools to gather and access HR data (Fecheyr-Lippens et al. 2015). New solutions for employee engagement, well-being and health enable companies to apply real-time analyses and derive conclusions by combining employee information with other organizational records, such as financial or customer data.

Nevertheless, benefits of REIS can only be generated if employees are willing to reveal sensitive information. On the downside, depending on the employer's framing of the need for persisting information in a system, it could be perceived by the employee as an information source enabling opportunistic behavior on behalf of the employer (Allen et al. 2007). Today, innovative technologies, databases, and the use of intelligent algorithms for big data analysis are enabling companies to analyze and understand information in a fast and comprehensive way (Stanton and Stam 2003). For example, implementing an expert system, as mentioned above, requires the willingness of employees to infer personal information about their skills, competencies, or projects. In a context of competitive pressure and the requirement of staff reductions, usage of automatic algorithms might then enable companies to identify expendable workforce (e.g., skills which are not required any longer). Similarly, data collected from the employee's enterprise social network usage could enable companies to control the behavior of their workforce (Brown and Lightfoot 2002; Jackson et al. 2007; Sewell and Barker 2006). Note that the organizations may not intend these possibilities at all, the question is whether employees subjectively misjudge their company's true (or future) intentions in the context of their personal framing of REIS.

It can be concluded that REIS can offer many benefits for all stakeholders, when it is applied and perceived in the intended way. However, several potential pitfalls might prevent stakeholders from using the system properly. As already stated, some potential difficulties coming along with REIS introduction and usage can be derived from existing psychological and IS theories. Therefore, the following subsection will explain the theoretical background of this research.

5.3. Theoretical Background

IS research has accumulated an impressive body of knowledge predicting and explaining system acceptance, usage, and success (e.g., Davis 1989; DeLone and McLean 2003; Venkatesh et al. 2003). A large stream of research has evolved around the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and their extensions (e.g., Davis 1989; Venkatesh and Bala 2008; Venkatesh et al. 2003). While these efforts have considerably broadened the perspective on an individual's usage of technologies, an aspect which

still requires attention is the quality or effectiveness of system use (e.g., Barki et al. 2007; Burton-Jones and Grange 2012; Burton-Jones and Straub Jr. 2006). This is especially relevant for information systems that are requesting sensitive information (REIS), since their value can only be derived when assessing the particular usage quality. If employees are providing false information, the actual value of REIS might not be achieved. The analysis of interviews in the qualitative study of Section 4 suggests the viability of synthesizing the Technological Frames Theory (Orlikowski and Gash 1994), insights from Privacy Calculus Theory (Dinev and Hart 2006) and the Psychological Contract Theory (Rousseau 1989). Since Privacy Calculus Theory and Technological Frames Theory have already been discussed exhaustively in previous sections (see Subsection 4.3) this subsection focuses on the explanation of the Psychological Contract Theory and its origin. All three theories help to explain how the relationship quality between an employee and an employer can determine how employees perceive REIS and therefore provide quality information within these systems. The Privacy Calculus Theory builds the basic frame of the research model and helps to explain the interaction between an employee's perceived benefits and his perceived vulnerability through information disclosure (see Subsection 4.3.1). Moreover, the Technological Frames Theory underscores the challenges arising from the employee's framing of technologies regarding the purpose and intention of the implementation of REIS between the company and its workforce. In particular, it helps to understand the employees' interpretation that an employer might act opportunistically and against the self-interest of employees. Finally, Psychological Contract Theory helps to explain how an employee's perceived relationship quality toward his or her employer determines which behaviors he or she expects from the organization and how these expectations can affect work-related behavior such as information system usage and information disclosure. Accordingly, all three theories serve as the basis for a model that explains the willingness of employees to submit information into REIS and other likely outcome behaviors when using such systems.

5.3.1. Brief Overview of Privacy Calculus Theory

Previous research has gathered considerable knowledge about how privacy concerns affect an individual's willingness to disclose sensitive data within information systems (e.g., Dinev et al., 2009; Malhotra et al., 2004; Krasnova et al., 2010). Thereby, research revolves around the idea that an individual's willingness to share personal information is influenced by the perceived costs and benefits of disclosing the data. In this context, trust, privacy risk, the sensitivity of data, legal regulations, and control play a crucial role in the decision-making process (e.g., Dinev and Hart, 2006; Dinev et al., 2009; Gerlach et al., 2015; Krasnova et al., 2010). As already found out in the previous section (Section 4) privacy concerns are of a different quality in an organizational setting as they do not involve the usually mentioned aspects like identity theft, or selling of data. In organizations, possible concerns arise as a result of users' dependencies on the employer and could range from unfavorable evaluations to layoffs.

5.3.2. Brief Overview of Technological Frames Theory

It is widely known that the acceptance and usage of information systems are depending largely on the perceptions of the information system user (Lin and Silva 2005). The Technological

Frames Theory gives a frame for the incongruence in perceptions and beliefs about technology implementation with regards to the main stakeholder groups in companies. Namely, the management, who is framing the strategy of the implementation, the employee, who is representing the user group, and the IT expert who is responsible for the implementation from the technological point of view (Orlikowski and Gash 1994). Furthermore, technological frames are characterized by three dimensions. (1) The technology strategy, representing the perceived goals and motivations of the employer behind the implementation; (2) the nature of the technology, referring to the people's understanding of the functionality and abilities of a system; and (3) the usage of technology, representing the understanding of how the benefits and consequences of usage are perceived (for more information see subsection 0 'The increasing importance of ESS has been exhaustively discussed among researchers (e.g., Kügler et al. 2015; Kügler, Smolnik, and Raeth 2012; Raeth, Kügler, and Smolnik 2011), and the implementation and usage have become pervasive within companies (Leonardi et al. 2013). Furthermore, research has shown that ESS exert powerful effects on the way internal collaboration takes place and how companies communicate and interact with external stakeholders (McAfee 2006). Although ESS have received increasing attention in recent years, research regarding antecedents and outcomes of effective ESS use is still sparse. Nevertheless, a few studies examining the use of ESS among employees exist (e.g., Herzog et al. 2013; Kügler and Smolnik 2014; Larosiliere and Leidner 2012; Wattal et al. 2010).

While these studies provide promising first insights, their majority are focused on measuring the success of ESS usage. As a valuable starting point, Kügler and Smolnik (2014) propose a conceptualization of usage modes for ESS. Along these lines, Herzog et al. (2013) examined the success of ESS by analyzing the methods and metrics applied by organizations, which served as measures for the usage of ESS by employees. Kügler and Smolnik (2013) investigate the benefits associated with ESS use for employees. The authors propose that ESS can increase employees' efficiency, affect their connectedness, support decision-making performance, and also increase innovative performance. In the same vein, a study regarding organizational Facebook use showed that organizational identification can be increased through ESS use by the organization's members (Larosiliere and Leidner 2012). Furthermore, Buregio, Maamar, and Meira (2015), as well as Williams et al. (2013), identified potential benefits and risks for companies and employees when using ESS. For instance, ESS enable quicker resource access but can simultaneously cause an overload of information (Buregio et al. 2015).

Research on the adoption of ESS aims to identify best practices and factors that influence the end-user adoption of ESS (Alimam et al. 2015). Regarding possible antecedents of ESS use and acceptance, Kügler et al. (2012) provide a first draft of a theoretical framework on how the acceptance of ESS could be examined. The authors suggest that the use of ESS might be influenced by organizational climate as well as by social and technical factors. Wattal et al. (2010) examined the use of organizational blogs by employees and found that network externalities and feedback from other users as recognition are crucial for the motivation to use enterprise blogs. Even though previous IS research irrevocably showed that privacy concerns are

a major influencing factor for the provision of personal information in SNS, there is a lack of research on this phenomenon in the organizational context.

In sum, extant research on organizations' implementation of ESS and the employee's use thereof has largely focused on outcomes of these systems (e.g., Herzog et al. 2013; Kügler and Smolnik 2013; Larosiliere and Leidner 2012). However, it is necessary to understand the reasons for and origins of the employee's privacy concerns about ESS, and thus the success factors for such technologies within organizations. As will be outlined below, incongruence in technological frames between employees and their employer play a central role in understanding the employee's beliefs about ESS, and thus their behavioral consequences and demands toward the company.
Technological Frames as Conceptual Framework').

For the present context the identified domains and related main stakeholders (in particular the employee) when implementing IT in a company, help to explain influencing factors and outcomes of the usage of REIS in companies. This indicates that employees who are using REIS, and are presenting the key stakeholder group for the success of the system, might perceive the system as a threat or negative change even though the company's actual goal of the implementation would be positive and not for the disadvantage of an employee. This might have an impact on the outcomes and usage of the system by the employee. In this context it is important to better understand the relationship between the employee and the employer, and what is driving the suspicions of employees. Therefore, the Psychological Contract Theory can explain how and why employees are trusting or distrusting their employer, based on experiences from the past.

5.3.3. The Psychological Contract Theory

In an organizational context, the relationship quality between an employee and his or her employer depends greatly on the psychological contract held by the individual employee (e.g., Morrison and Robinson 1997; Rousseau and McLean Parks 1993; Robinson 1996; Rousseau 1989). It refers to an employee's perception of what he or she owes to the employer and what the employer owes to the employee (e.g., Morrison and Robinson 1997; Robinson 1996). Furthermore, it presents a rather broad concept and obligations perceived in this regard must not be based on formal contracts, but can also result from an employee's subjective perceptions and implicit conclusions (Morrison and Robinson 1997). The quality of such contracts helps to explain what employees expect from their organizations (and what not). In this regard, breaches of psychological contracts significantly determine the employee's work-related attitudes and behaviors (e.g., Restubog et al. 2013; Robinson 1996; Zhao et al. 2007). In environments with increasing turbulence and uncertainty, trends such as downsizing, restructuring, and reliance on temporary workers can influence psychological contracts (e.g., Morrison and Robinson 1997). The resulting emotional state of perceived violation of a psychological contract decreases trust toward the employer and, as a consequence, reduces an employee's contributions to the organization (Morrison and Robinson 1997; Robinson 1996).

As this research deals with a privacy calculus in the organizational context, and its peculiarities coming from the assumption that the employer-employee relationship shapes this calculus, the perceived breach and resulting violation of the psychological contract of the employee plays a significant role. The perceived breach and violation of a psychological contract can explain the quality of the respective relationship of the employee with his employer (e.g., Morrison and Robinson 1997; Rousseau and McLean Parks 1993; Robinson 1996; Rousseau 1989). As Rousseau (1989) stated, the breach and violation of the psychological contract are the link between the contract itself and possible resulting behaviors. To get a better understanding of the relation of the psychological contract, its breach, and associated violation to PIBV, a precise definition of the development, the breach, and the violation of the psychological contract are given.

The Psychological Contract

The first time the psychological contract has been mentioned in the context of the working environment was in 1960 by Argyis (cited after Conway and Briner 2005). He stated that employees and their employer develop psychological contracts to state their expectations towards the fulfillment of their mutual needs. For example, if employees perceive that they have the opportunity for growth and feel that their initiative and engagement is respected, they will in return respect the right of the company for development. Morrison and Robinson (1997, p. 229) define the psychological contract as *'an employee's beliefs about the reciprocal obligation between that employee and his or her organization, whereas these obligations are based on perceived promises and are not necessarily recognized by agents of the organization.*' This definition comprises several interesting peculiarities that the psychological contract owns.

One aspect is the belief of an employee, which is generating the psychological contract. These beliefs are ideas regarding promises and obligations that an employee has, concerning his work life and the behavior of the employer (Morrison and Robinson 1997). Furthermore, obligations in a psychological contract can include a broad range of implicit elements, which are resulting from the interpretation of behavioral patterns of past exchange processes or observation (Robinson and Rousseau 1994). Those elements can be regular pay, and other short-term benefits, but also more social and relational items such as loyalty, fairness, trust, or support *'through sickness and in health'* (Rousseau and McLean Parks 1993, p. 12). Psychological contracts are always referring to the perceived exchange agreement of an employee, whereas the perception of this agreement is decisive. It is not necessarily an agreed exchange but the employee's beliefs that agreement regarding the contract is given, even though there must not be an actual accordance where both parties have the same understanding of the contract (Robinson and Rousseau 1994). When discussing the perceived exchange agreement among two parties, it is also important to state who these two sides are representing. It is easy to identify the employee as one party of the contract, whereas the other party is a more abstract construct – the employer. It is not easy to say who or what is perceived as the construct employer by the employee and therefore it is at the same time hard to say that this party is holding a psychological

contract. Especially when it is perceived as the abstract organization itself, which is not representing a human being. On the contrary, if a manager is representing the perception of the employer it is possible that this party can develop a psychological contract. Nevertheless, it is hard to point out who is representing this party in the perception of the employee. In conclusion, Robinson (1989) stated that only the employee can uphold a psychological contract as a human being. Furthermore, psychological contracts are perceptual in nature and not necessarily shared by different actors within the organization (Rousseau 1989). Even though items of the exchange process seem to be objective, they might be subjective interpretations of the employee. This fact makes it difficult to materialize or understand a psychological contract (Conway and Briner 2005).

The Breach and Violation of the Psychological Contract

There are several keys in the definition of the psychological contract, which play a significant role for the understanding of the perception of an employee that such a contract is broken or even violated by the employer. For employers and researchers, it is not only important to get an understanding of how a contract is developed but even more important to understand how the perception of a breach of the contract and a related emotional reaction of resentment and betrayal of the employee occurs (Robinson and Morrison 2000). Those reactions lead to behavioral changes of employees and therefore are the real challenge when discussing the psychological contract (Robinson and Morrison 2000). Thus, a breach of the psychological contract is defined as an employee's *'cognition that one's organization has failed to meet one or more obligations within one's psychological construct in a manner commensurate with one's contributions'* (Morrison and Robinson 1997, p. 230). Moreover, the violation of a psychological contract is defined as an affective or emotional state that may or may not accompany the perception of the psychological contract breach (Robinson and Morrison 2000). In the following, the breach and violation of the psychological contract will be illustrated and explained.

In literature, two root causes of a contract breach have been identified – reneging and incongruence (e.g., Morrison and Robinson 1997; Robinson and Morrison 2000). Whereas reneging is present, when a representative of a company knows that a commitment on behalf of the employer is existing but is failing to meet the commitment on purpose. For example, a recruiter is making concessions in the recruitment process and afterwards is failing to uphold the concessions. Incongruence is present when an employee and the representative of the company have different perceptions about a given concession or the composition of a given concession. In this case, an example could be when an employee is misperceiving a statement made by a recruiter in the recruitment process. Due to a resulting discrepancy between an employee's interpretation of what has been promised and his perception of what he actually received, both scenarios would lead to a perception of psychological contract breach. Related to reneging and incongruence, several situations and scenarios can influence the perception of a psychological contract breach (Robinson and Morrison 2000). For instance, a breach will be more likely if a company's performance is declining or has fallen short of what was expected. In addition to that, an employee's performance can also influence the breach, as the employment

relationship is based on reciprocal obligations. When an employee is not maintaining his side of the contract this might lead to reneging on behalf of the employer. This perceived opportunistic behavior from the perspective of the employee might, in turn, lead to a perceived contract breach on behalf of the employee. On the other hand, if an employee has been part of a formal socializing process within the company or had extensive interaction with representatives of the company previous to their hiring, the perception of contract breach might be lower. Furthermore, a perceived psychological contract breach is more likely to occur, the longer the relationship endures and the stronger a reciprocal exchange happens (Rousseau 1989).

Even though the described situations might lead to a perception that a psychological contract is broken, they not necessarily result in the perception that a contract is violated (Robinson and Morrison 2000). This intense emotional reaction following the psychological contract breach depends on a subjective interpretive process by which an employee attributes value and meaning to the perception of the breach. A perceived breach is more likely to result in perceived violation if an employee is attributing the breach to reneging rather than to incongruence under perceived unfair conditions (Robinson and Morrison 2000). This means that employees are more likely to have intense emotional reactions, such as a decrease in trust and respect, lower job, and organizational satisfaction, as well as an increased intention to quit (Robinson and Rousseau 1994).

It can be concluded that the PIBV of an employee might be influenced by the quality of the employer-employee relationship, which is reflected in the psychological contract breach and violation. In the following these constructs will be incorporated in a theoretical model as sources of perceived information-based vulnerability.

5.4. Frame of Reference of the Study

As already stated this study focuses on the antecedents and outcomes of the perceived information-based vulnerability of employees when using REIS. To measure the related mechanisms, a research model was developed and examined. It starts with influencing factors derived from the nature of the system and the employer-employee relationship. The antecedents lead to a mediating construct PIBV that reflects the mechanisms induced by expectations of opportunistic behavior with regard to a system and thus synthesizes and transfers its antecedents' effects on its outcomes (see Figure 9). The expected outcomes are the disclosure intention of employees or the opposing effect of resistance, reflected in three different stages.

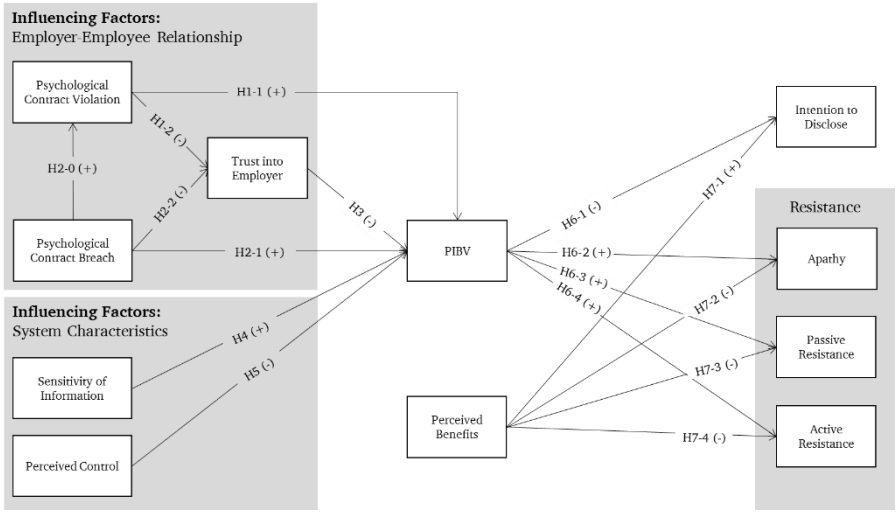


Figure 9: Theoretical Framework

As Orlikowski and Gash (1994) already stated, negative interpretations of the nature of technology, technology strategy, and usage may result in wrong expectations, inconsistent actions, resistance, suspicion, and limited use of the technology. These frame characteristics are reflected in the influencing factors of PIBV and the perceived benefits of a REIS. It can be assumed that the calculus of benefits and PIBV is influencing the decision of employees to resist or contribute to REIS. An employee's perception of system benefits, the nature of a system and the implementation strategy of a company have an impact on resulting expectations and actions regarding the system (e.g., Davidson 2006; Mishra and Agarwal 2010; Olesen 2014; Orlikowski and Gash 1994). Therefore, to determine the extent of a user's adoption or resistance against REIS, it is necessary to understand an employee's perception of REIS and their related PIBV. As found in the previous section (Section 4), trust and negative experiences have an impact on an employee's technological framing and their intention to disclose information. It can be assumed that the breach and violation of the psychological contract, reflecting the experiences with the employer, have a direct impact on an employees perceived PIBV. Furthermore, the breach and violation contribute to the trust relationship between an employee and his employer, which in turn also has an impact on PIBV. The model assumes that trust serves as a mediator in the relationship between PIBV with the psychological contract breach and the psychological contract violation. Due to distrust and bad experience, an employee might be more uncertain whether information revealed within the system will be used by the employer to monitor its employees. In contrast, in the presence of a high-quality psychological contract, the expectation that their information submitted in this system is treated respectfully and in mutual interest would be higher. As long as an employee believes that the employer is upholding his side of the psychological contract, he or she might be more willing to provide revealing information within these systems.

Not only the employer-employee relationship and the related perceived implementation strategy are crucial for the usage of the system and the technological frame. The functionality and benefits in the day-to-day business are also linked with the framing (Orlikowski and Gash 1994). Thus, it is assumed that factors concerning the functionality, such as sensitivity of the requested information and perceived control have an impact on an employee's PIBV as well.

5.5. Derivation of Research Hypotheses

In the following section, the conceptual framework is presented. The framework centers on the construct PIBV and illustrates antecedents and outcomes, which are important from the perspective of Privacy Calculus Research, Technological Frames, and Psychological Contract Theory. To achieve a good understanding of how the employer-employee relationship and related factors have an impact on an employees perceived vulnerability when using REIS, it is important to focus on important influencing factors, which are particularly relevant from the perspectives of Technological Frames and Psychological Contract Theory.

5.5.1. Perceived Information-Based Vulnerability

As argued above, the success of REIS depends strongly on the quality of information a user enters into these systems. In turn, an employee's choice to make information available which possibly reduces information imbalance for the employer is affected by the user's anticipation of the implementation intention of the employer. Based on the Privacy Calculus' notion of privacy concern (e.g., Dinev and Hart 2006; Dinev et al. 2008; Xu et al. 2008), the user's perception of information-based vulnerability (PIBV) of a system is defined as the extent to which a system evokes an employee's fear that information entered into the system could be used in an opportunistic manner by the employer. PIBV presents a perceived system characteristic which reflects a given user's strength of belief that making information available in the system could backfire at some point in time. An information system which only requires an employee to enter sales orders might exert a low degree of PIBV as the sales information does not reveal any characteristics or behaviors about the employee. In contrast, an enterprise social networking tool in which a user's contributions and group discussions are linked to a personalized account could be associated with increased PIBV as it could make the content of the employee's conversations transparent. For instance, personal weaknesses, activities, tendencies, or work habits could become tangible for the employer, even though this was not intended by the employee.

Overall, PIBV should be context specific and dependent on the employee's interpretations and perceptions of the nature of the system in focus, the experiences with the employer and the related purpose of the implementation of the system (Orlikowski and Gash 1994). Due to context changes, PIBV might also vary over time. For instance, at a given time, a company might be in a stable situation without pressure to save costs. However, the need for exploiting information about the employee's skills and behaviors could be bigger when economic pressure forces the company to reduce costs. In this new context, employees might fear that the economic pressure could lead to layoffs. Therefore, an employee might conclude that the company's need for

information about its workforce is higher – implying higher suspicion by the employee and an increase in PIBV.

5.5.2. Influencing factors on PIBV

The actual cause why employees' PIBV might increase with regard to a system can be due to technological framing and related influencing factors causing the employee's frame, such as trust and past experiences. When employees perceive the implementation purpose, the nature of the system or the usage of the system as a negative change or threat, they might not use the system (Orlikowski and Gash 1994). Since the information stored within REIS offers the possibility to draw conclusions about workplace behaviors and attitudes, location, or performance, employees might perceive this nature as a reason that the technology strategy of the company could be different from the communicated one. They could fear that their employer might use the offered information in an opportunistic manner and against the employee. This fear can even be increased by negative experiences regarding fair treatment and fulfillment of expectations by the employer. It is assumed that the perception whether the employer might misuse the offered information is greatly dependent on the employer-employee relationship. Going further, the antecedents of PIBV are a) contingent on the quality of the employer-employee relationship, and b) depending on the system's characteristics.

Psychological Contract Breach and Violation

First, breaches of an employee's psychological contract and the related emotional reaction of perceived violation (Robinson and Rousseau 1994) should significantly influence the employee's PIBV. The perceived implementation strategy of the company plays a significant role in the system framing of employees. This perceived strategy highly depends on the experiences of the employee with his employer and their mutual relationship (Orlikowski and Gash 1994), which is reflected in the perceived breach and violation of the psychological contract. Based on Morrison and Robinson (1997), the breach of the psychological contract is defined as the perceived failure of the employer to meet one or more obligations within one's psychological construct proportionally to one's contributions. Furthermore, the violation of the psychological contract is understood as affective or emotional states that may or may not accompany the perception of the psychological contract breach and follow from the employee's conviction that the employer has not adequately upheld the psychological contract (Robinson and Morrison 2000). Ring and Van de Ven (1994) underline that those perceptions of failure and resulting fairness decrease are linked to uncertainty about opportunistic behavior in an exchange relationship. For example, if a company is known for poor treatment of its workforce, an employee will have a lower basic expectation of trust, mutuality, and honest behavior (Robinson and Rousseau 1994). Otherwise, if a company has historically adopted principles such as reliability and concern for its staff, employees will have higher expectations for fairness, mirrored in the psychological contract (Morrison and Robinson 1997) and therefore PIBV should be lower. Employees who have felt that their psychological contract is broken or violated will adjust their beliefs accordingly (Restubog et al. 2013). For instance, if companies already make use of surveillance software to monitor their workforce, employees might feel that the moral border to

additionally use data from REIS to satisfy their information need might be relatively low. Users who have experienced a breach or even a violation of their psychological contract might also report higher values of PIBV. In the present study, both relations will be tested and hypothesized. It can be expected that the breach and the violation of the psychological contract have an impact on the PIBV of REIS users. As the breach of a contract can exist without the perception of violation following this breach, the goal of these hypotheses is to find out whether the breach of a contract is sufficient for employees to perceive information-based vulnerability, independently from the feeling of violation. The resulting hypotheses are as follows:

H2-0: A perceived psychological contract breach by a REIS user will increase his or her perceived psychological contract violation.

H2-1: A psychological contract breach perceived by a REIS user will increase his or her perceived information-based vulnerability of a system.

H1-1: A psychological contract violation perceived by a REIS user will increase his or her perceived information-based vulnerability of a system.

Trust into Employer

People desire to be in a trustworthy environment (Bansal et al. 2010). Trust reduces the concern that the employer might act inappropriately. The positive utility of trust into the employer might be negatively impacted by the violation or breach of the psychological contract of an employee (Robinson and Morrison 2000). The degree to which trust characterizes the employment relationship will furthermore influence the PIBV of REIS. As already found in several other studies, trust positively influences the behavioral intention of people by decreasing privacy concerns (e.g., Culnan and Armstrong 1999; Taddei and Contena 2013). Trust, as conceptualized in this research in alignment with Psychological Contract Research, is assumed to create a positive employer-employee relationship and therefore decreases the concern for vulnerability through information-disclosure, which in turn increases the employee's intention to disclose. Indeed, trust into the employer can be described as anticipations or beliefs concerning the probability that future actions of the employer are favorable – or at least not harmful – to personal interests (Morrison and Robinson 1997). This type of trust is mainly based on experiences made in the past (Morrison and Robinson 1997). For instance, employees who experienced a contract breach or even violation of the contract within their actual employment relationship or in a previous employer-employee relationship might have a tendency to trust less into their employer (Robinson 1996). Therefore, the lower the trust of an employee into his employer, the more likely the employee expect opportunistic behavior and therefore higher PIBV of REIS. Accordingly, trust is hypothesized to have a negative impact on PIBV. As the trust of employees is significantly impaired by the prior contract breach and accompanied emotional reaction of violation, it can be hypothesized that employees perceive a higher fear of opportunistic behavior in the future (Deery, Iverson, and Walsh 2006). Hence, trust is also hypothesized to mediate, in any way, psychological contract breach and violation with PIBV.

H3: Higher trust into the employer will decrease a user's perceived information-based vulnerability of a system.

H1-2: Trust into the employer mediates the relationship between psychological contract violation and PIBV.

H2-2: Trust into the employer mediates the relationship between psychological contract breach and PIBV.

Sensitivity of Information

Research investigating information privacy in online consumer settings suggests that the perceived sensitivity of information requested by a system, significantly influences an individual's decisions to provide personal information items (e.g., Malhotra et al. 2004; Phelps et al. 2000). Perceived sensitivity of information is defined as *'a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent'* (Dinev et al. 2013, p. 302). In this research, the external agent is understood as an information system hosted by the employer, which might or might not have the nature to require sensitive information. As known from Technological Frames Theory, an employee's perception of a system is, among others, depending on the nature of the information system (e.g., Jackson et al. 2007; Olesen 2014; Orlikowski and Gash 1994). The degree of sensitivity of the demanded information is attributed to this nature of technology (see Section 4), which includes how a system is designed and perceived by a stakeholder. Therefore, the perceived sensitivity of information should have a significant impact on the positive or negative frame shaping of employees. If employees have a negative technological frame, they withhold sensitive information to protect themselves from opportunistic actions of the company, promoted by their information disclosure. Therefore, it can be expected that the same holds true for the release of information within REIS. The more information solicited by a system is perceived as sensitive by the employee, the higher the perceived potential damage if information is opportunistically used by the company. Thus, higher degrees of perceived information sensitivity should increase the user's PIBV.

H4: Higher perceived sensitivity of information required from REIS will increase a user's perceived information-based vulnerability of a system.

Perceived Control

In addition, information privacy research suggests that perceptions of privacy and the disclosure of personal information are significantly determined by an individual's perceptions of control retained over their information (e.g., Dinev et al. 2013; Krasnova et al. 2010; Phelps et al. 2000). This is also supported by the theory of Technological Frames, as the nature of the system, which also reflects the degree of control over information (see Section 4) – plays a significant role in the frame shaping of stakeholders. If the nature of a system is perceived as poor, the result might

be a higher degree of fear towards the misusage of provided information. Therefore, the perceived control over inserted information plays a crucial role in the frame shaping of REIS by an employee and hence the perception of PIBV when using the system. Perceived control is defined as an *'individual's belief in his or her ability to manage and release the dissemination of personal information'* (Xu et al. 2011, p. 804). Furthermore, an employee's fear of potential opportunistic behavior associated with PIBV might not exclusively relate to the present situation alone. Rather, the employee could believe that information disclosed within a system could be misinterpreted in the future when taken out of context. Therefore, an employee should feel less vulnerable if he or she retains control over the information being able to modify or delete it at any given point in time. Being able to monitor the dissemination of provided information might lead to the perception that a system has an employee friendly nature. Therefore, the technological frames perspective supports the proposition that higher perceptions of control might reduce PIBV.

H5: Higher perceptions of control over information entered into REIS will decrease a user's perceived information-based vulnerability of a system.

5.5.3. Consequences of Perceived Information-Based Vulnerability

A user's PIBV should be strongly related to outcomes that can characterize the quality of REIS usage, based on the Technological Frames and Psychological Contract Theory, as well as Privacy Calculus Research. The Technological Frames Theory indicates that employees might perceive information systems as a threat, which in turn might have an impact on the usage of these systems (Orlikowski and Gash 1994). They state that negative frames may result in incorrect anticipations, unpredictable actions, resistance or limited use of the system (Orlikowski and Gash 1994). Furthermore, results from Psychological Contract Theory indicate similar behavior of employees towards the company when they feel that their contract was violated. People who feel a violation of the psychological contract may react with decreased citizenship behavior or lower motivation. In extreme cases of violation, employees might even seek for revenge or engage in destructive behavior (Morrison and Robinson 1997). When transferring this resulting behavior to the recent research context, it could be expected that employees might not be motivated to use the system or even react with more extreme behaviors, such as bad mouthing REIS. In conclusion, if employees perceive high degrees of information-based vulnerability and low benefits two types of outcomes seem to be particularly relevant: decrease of usage activities and resistance.

Intention to Disclose Information

First, an employee's perception that REIS might be implemented for a different strategic purpose than communicated (Orlikowski and Gash 1994), as for example using inserted information for opportunistic actions, should cause them to interact accordingly and more cautiously with these systems. As illustrated above, REIS depends on user's contributions of honest content such as

feedback, comments, or helpful suggestions. By their nature, employees' input of quality information into REIS may be hard to enforce, and the honesty of information may be hard to verify if they have the perception that the strategic purpose of REIS is to their disadvantage. Research on B2C contexts such as e-commerce or online social networks has found that users' fear of opportunistic behavior of an opponent party will greatly decrease their intention to provide personal information (e.g., Dinev and Hart 2006; Li, Sarathy, and Xu 2010; Okazaki, Li, and Hirose 2009; Son and Kim 2008). In an organizational context, research suggests that the employee's honest contributions, extra-role behaviors, and behaviors that indicate that they responsibly participate in or are concerned about the life of the company are affected by the quality of psychological contracts (Morrison and Robinson 1997; Robinson 1996; Rousseau 1989). It can be expected that REIS usage and the provision of quality information should strongly depend on a user's PIBV of a system. In this case, employees might only use a system to the extent which is necessary but avoid entering honest information which can help improve their work and life, the work of others or the company as a whole. In this research, the employee's intention to disclose is defined as the voluntary and intentional exposure about oneself to the employer through enterprise information systems (based on Posey et al. 2010).

H6-1: Higher perceptions of information-based vulnerability of REIS will decrease a user's intention to disclose information.

Resistance

Finally, due to the possible relation to psychological contract breaches and the underlying assumptions of the Technological Frames Theory – higher PIBV should also lead to resistance behavior such as rejecting usage, undermining the system's benefits, or badmouthing (Lapointe and Rivard 2005). Especially, when there is a negative frame perception of a system, it might result in resistance (Orlikowski and Gash 1994). As Restubog et al. (2013) point out, employees who feel that their psychological contract was broken might engage in deviant behavior. Furthermore, violations of the contract are often associated with strong emotional reactions such as anger (Morrison and Robinson 1997; Zhao et al. 2007). Overall, employees' higher PIBV imply that they fear that information might be used against them. Technologies which are perceived as a threat are subject to resistance by its users (Lapointe and Rivard 2005; Markus 1983; Orlikowski and Gash 1994).

Resistance behaviors on behalf of the employee can range from a simple rejection of usage to a deviant behavior which can harm a company's success (Lapointe and Rivard 2005). Resistance against REIS can be divided into four different levels. (1) *Apathy* by showing distance and lack of interest towards a system, (2) *passive resistance* by only providing necessary information without extra effort or finding excuses to not use a system, (3) *active resistance* by – additionally to passive resistance – articulating negative opinions towards a system to co-workers, or even (4) *aggressive resistance* by sabotaging or rebelling against a company (Lapointe and Rivard 2005). Even though there are four stages of resistance further research and operationalization

of items will show that the fourth stage of resistance – aggressive resistance – will be excluded from this study, as it is not relevant for the present context. For instance, an employee might express resistance against REIS as he might want to protect himself or might try to sabotage the implementation to harm his company (Restubog et al. 2013). The lowest degree of resistance – *apathy* – might lead to the consequence that employees only insert necessary information but would not seriously deal with the system. They would not fully engage by inserting truthful and complete information. The next higher degree of resistance is the simple but effective rejection of REIS – *passive resistance*. Rejection and therefore, withdrawal of a system makes it useless. Hence, if it is a lower degree of resistance, employees might not have an opposite view towards the system but might not see sense to use it. Moreover, even if they have negative opinions, they might not mention their view to others. On the other hand, if the degree of resistance is getting higher, employees might try to build alliances against the system or even try to sabotage the implementation process and the system itself (Lapointe and Rivard 2005). When an employee's resistance level is expressed by criticizing the system in front of other colleagues or speaking badly about the employer's purpose of implementing such a system, this is reflected in *active resistance*. In such a situation other colleagues might adopt the opinion and also resist the usage. Hence, active resistance would lead to undermining of the potential benefits of REIS (Lapointe and Rivard 2005).

Again, due to the nature of REIS, employees might have a high PIBV and as an outcome react with a degree of resistance. This could result in incorrect or imprecise information, no information at all, or people fighting against the system. This would sabotage the original purpose intended by the system. Therefore, it is expected, that higher PIBV should result in higher degrees of resistance.

H6-2: Higher perceptions of information-based vulnerability of REIS will increase a user's degree of apathy towards the system.

H6-3: Higher perceptions of information-based vulnerability of REIS will increase a user's degree of passive resistance towards the system.

H6-4: Higher perceptions of information-based vulnerability of REIS will increase a user's degree of active resistance towards the system.

5.5.4. Benefits of Revealing Enterprise Information System Usage

The Privacy Calculus Theory posits that disclosure of sensitive information happens when the expected benefits from disclosure outweigh the perceived costs (Dinev and Hart 2006). It is known that Internet consumers are purchasing on the Web when they perceive many benefits, as cost savings, time savings, and increased variety of products compared to traditional shopping (Kim et al. 2008). The same applies to SNS users. They tend to submit more information when they think that they perceive any kind of benefit, such as enjoyment, relationship maintenance, or relationship building (e.g., Hollenbaugh and Ferris 2014; Krasnova and Veltri 2010). Consequently, it can be anticipated that the same holds true for employees when participating in REIS. In contrast to PIBV, which is a potential barrier to disclose honest information and a

driver of resistance, an employee's perceived benefit should be a major incentive for disclosing information and inhibitor of resistance against REIS. According to that, perceived benefits are defined as an employee's belief about the extent to which he or she will become better off from using the system (Kim et al. 2008, p. 547). Thus, the more employees perceive benefits related to disclosure, the more likely they are willing to disclose, and the less they will try to resist against the system and do badmouthing. Consequently, it can be expected that the perceived benefits of disclosure in REIS have a positive impact on the user's intention to disclose information, and a negative impact on resistance.

H7-1: Higher perceived benefits when using REIS will increase a user's intention to disclose information.

H7-2: Higher perceived benefits when using REIS will decrease a user's apathy towards the system.

H7-3: Higher perceived benefits when using REIS will decrease a user's passive resistance towards the system.

H7-4: Higher perceived benefits when using REIS will decrease a user's active resistance towards the system.

5.5.5. Overview of Research Model

In this section the hypotheses for the research model were developed. It was outlined how PIBV should serve as a potential inhibitor for sensitive information disclosure intentions of employees and at the same time increase the resistance behavior of the workforce against REIS. Furthermore, the countermeasure *Perceived Benefits* was explained and hypothesized on how it might outweigh the fear of opportunism of employees.

Construct	Definition
Sensitivity of Information	*'A personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent'* (Dinev et al. 2013, p. 302).
Control	An *'individual's belief in his or her ability to manage and release the dissemination of personal information.'* (Xu et al. 2011, p. 804)
Psychological Contract Breach	The perceived failure of the employer to meet one or more obligations within one's psychological construct proportionally to one's contributions. (based on Morrison and Robinson 1997, p. 230)
Psychological Contract Violation	An affective or emotional state that may or may not accompany the perception of the psychological contract breach. (based on Morrison and Robinson 1997, p. 230)

Construct	Definition
Trust into Employer	Trust into employer is described as anticipations or beliefs concerning the probability that future actions of the employer are favorable – or at least not harmful – to the employee's interests. (based on Morrison and Robinson 1997, p. 238)
Perceived Information-Based Vulnerability	Perceived information-based vulnerability captures a user's perceptions that information entered into a system can be used in an opportunistic manner by the employer. (self-developed)
Benefits	Perceived benefit is an employee's belief about the extent to which he or she will become better off from using the system. (based on Kim et al. 2008, p. 547)
Intention to Disclose	An employee's voluntary and intentional exposure about oneself to their employer through enterprise information systems (based on Posey et al. 2010)
Apathy	*'Apathy or indifference which can be labeled a neutral or transition zone, characterized by a lack of positive or negative emotions or attitudes (indicated by no demonstrated interest).'* (Coetsee 1999, p. 210)
Passive Resistance	*'Passive resistance exists when mild or weak forms of opposition to change are encountered, demonstrated by the existence of negative perceptions and attitudes expressed by voicing opposing views, regressive behavior such as threats to quit or voicing other indications of the rejection of change.'* (Coetsee 1999, p. 210)
Active Resistance	*'Active resistance is typified by strong but not destructive opposing behavior such as blocking or impeding change by voicing strong opposing views and attitudes, working to rule, slowing activities down, protests, and personal withdrawal.'* (Coetsee 1999, p. 210)

Table 13: Overview of Constructs in the Research Model

For an overview, Table 13 again illustrates all constructs of the derived model and their related definitions. Moreover, the resulting research hypotheses of the research model are summarized in Table 14. An illustration of the hypotheses and latent constructs can be found in Subsection 5.4, where the frame of reference of this research is explained (Figure 9).

H#	Hypotheses
H1-1	A psychological contract violation perceived by a REIS user will increase his or her perceived information-based vulnerability of a system.
H1-2	Trust into the employer mediates the relationship between psychological contract violation and PIBV.
H2-0	A perceived psychological contract breach by a REIS user will increase his or her perceived psychological contract violation.
H2-1	A psychological contract breach perceived by a REIS user will increase his or her perceived information-based vulnerability of a system.
H2-2	Trust into the employer mediates the relationship between psychological contract breach and PIBV.
H3	Higher trust into the employer will decrease a user's perceived information-based vulnerability of a system
H4	Higher perceived sensitivity of information required from REIS will increase a user's perceived information-based vulnerability of a system.
H5	Higher perceptions of control over information entered into REIS will decrease a user's perceived information-based vulnerability of a system
H6-1	Higher perceptions of information-based vulnerability of REIS will decrease a user's intention to disclose information
H6-2	Higher perceptions of information-based vulnerability of REIS will increase a user's degree of apathy towards the system.
H6-3	Higher perceptions of information-based vulnerability of REIS will increase a user's degree of passive resistance towards the system.
H6-4	Higher perceptions of information-based vulnerability of REIS will increase a user's degree of active resistance towards the system.
H7-1	Higher perceived benefits, when using REIS will increase a user's intention to disclose information.
H7-2	Higher perceived benefits, when using REIS will decrease a user's apathy towards the system.
H7-3	Higher perceived benefits, when using REIS will decrease a user's passive resistance towards the system.
H7-4	Higher perceived benefits, when using REIS will decrease a user's active resistance towards the system.

Table 14: Overview of Hypotheses

5.6. Methodology of Data Analysis

In the following, the previously defined research hypotheses are going to be tested by conducting a survey analysis with potential system users. The Data has been collected between March and July 2016. For the analysis of the collected data, a covariance analysis has been applied as methodology to validate the structural equation model. In the following, the covariance analysis will be described, and subsequently, the operationalization of the latent variables as well as the

data collection process will be presented. In the end, the theoretical framework will be evaluated, and the hypotheses will be examined.

5.6.1. The Covariance Analysis

For the examination of complex relationships, it is common to use a causal analysis as methodology. It allows to simultaneously estimate the validation of the effect mechanisms of a model (Jarvis, MacKenzie, and Podsakoff 2004). The benefit of this approach is that causal effect chains, such as '*A influencing B influencing C*', can be analyzed simultaneously. Based on correlative relationships between latent variables, the causal analysis is examining and quantifying causalities from experimental and non-experimental data. In the center of the statistical examination is the non-denial of hypotheses derived from a logically justified model of effect structures, by analyzing empirical data. Thus it allows the analysis of causally dependent relationships between multiple variables, which can only be measured indirectly. In general, depending on the goal of the analysis, there are two different approaches to examine a structural equation model – a variance or covariance causal analysis (Gefen, Straub, and Boudreau 2000).

The focus of the data analysis is the assessment of how good the theoretical framework is describing the empirical observations, and therefore, the verification of the goodness-of-fit of the underlying theoretical model. For this objective, it is recommended by scientific literature to apply a covariance analysis (e.g., Gefen et al. 2000; Herrmann, Homburg, and Klarmann 2008). A covariance analysis is applied to estimate causal relations in structural equation models with latent variables (Herrmann et al. 2008). By conducting a covariance analysis on a given data set, one can show that the assumed research model with all paths is plausible and supported by the data (Gefen et al. 2000). If you want to examine the explanatory power of certain factors of the theoretical model for one or multiple target constructs, it is recommended to apply a variance analysis, which is also called a partial least square (PLS) estimation (e.g., Gefen et al. 2000; Herrmann et al. 2008). In the PLS approach, it is possible to conclude about the explained variance of the endogenous latent variables (Gefen et al. 2000). However, the goal of the following analysis is to prove that the operationalization of the theoretical model is confirmed by the collected data. According to that, the PLS approach can be eliminated and the covariance analysis is applied.

Global Goodness-of-Fit

To objectively assess whether a research model can be mapped to empirical data, different assessment criteria can be applied. The basic idea for the corresponding measures is the assumption that a fitting theory would represent a perfect reflection of the reality, and therefore the empirical covariance matrix would fit with the hypothesized covariance model (Gefen et al. 2000). Several measurement criteria can be used to measure the global goodness-of-fit. However, based on extensive simulation analyses four global goodness-of-fit statistics could be identified as particularly suitable (Herrmann et al. 2008; Hu and Bentler 1998, 1999). The four measures are classified into inferential, descriptive and incremental goodness-of-fit statistics,

whereas inferential and descriptive statistics are summarized as stand-alone goodness-of-fit measures. The classifications are characterizing the assessment approach of each statistic (Herrmann et al. 2008). Incremental statistics, such as the 'Comparative Fit Index' (CFI) as well as the 'Non-Normed Fit Index' (NNFI) [equivalent to 'Tucker-Lewis Index' (TLI)] are based on the χ^2-statistics and are assessing the proposed, relevant model in relation to a basic null model, where each indicator is specified as uncorrelated. The null model contains no information about the relevant model and therefore identified relations in the data set are considered as coincidence (Hu and Bentler 1998). Both measures consider the degree of freedom in the relevant model (index *r*) and the null model (index *b*) and show an acceptable goodness-of-fit when the values are higher than 0.9 (Hu and Bentler 1998). The degree of freedom *(df)* is applied to take the model complexity and sample size into account, and the relating formula is as follows: $df = \frac{1}{2}[(p)(p+1)] - k$, where p is the amount of indicator variables and k the amount of parameters to be estimated (Hair et al. 2006; Walker 1940).

Formally the two following equations are showing the CFI and NNFI measurement (e.g., Herrmann et al. 2008; Hu and Bentler 1998):

$$NNFI = \frac{(\frac{\chi_b^2}{df_b}) - (\frac{\chi_r^2}{df_r})}{\left(\frac{\chi_b^2}{df_b}\right) - 1}$$

$$CFI = 1 - \frac{\max\{\chi_r^2 - df_r; 0\}}{\max\{\chi_b^2 - df_b; \chi_r^2 - df_r; 0\}}$$

On the contrary to incremental goodness-of-fit measures, stand-alone goodness-of-fit statistics are not comparing the relevant model with a null model, but the absolute predictive power of the model with respect to the empirical covariance matrix (e.g., Herrmann et al. 2008). Stand-alone measures are classified into inferential and descriptive statistics for the evaluation of the adoption of the model (Herrmann et al. 2008). A common approach for the inferential goodness-of-fit statistics is the 'Root Mean Squared Error of Approximation' (RMSEA) and for the descriptive goodness-of-fit statistics the 'Standardized Root Mean Square Residual' (SRMR). For both measures, it is better to have small values for a good (≤0.05) and acceptable (≤0.10) fit of the model (Herrmann et al. 2008). The formulas for RMSEA and SRMR are as follows:

$$RMSEA = \left(\frac{\chi^2 - df}{df(n-1)}\right)^{1/2}$$

$$SRMR = \sqrt{\frac{2\sum_{i=1}^{q}\sum_{j=1}^{i}\left(\frac{s_{ij} - \hat{\sigma}_{ij}}{s_{ii}\, s_{jj}}\right)}{q(q+1)}}$$

Whereas q is the number of indicator variables, n the sample size, s_{ij} the element in column i and row j of the empirical covariance matrix s and or $\hat{\sigma}_{ij}$ the element in column i and row j of the covariance matrix $\sum(\theta)$ implied by the model (Herrmann et al. 2008). Table 15 summarizes the applicable criteria for the evaluation of the goodness-of-fit of the relevant model.

Type of Measure	Incremental		Stand-Alone	
Name	CFI	NNFI	RMSEA (Inferential)	SRMR (Descriptive)
Recommended Threshold	≥ 0.9	≥ 0.9	≤ 0.1	≤ 0.1

Table 15: Overview of Global Goodness-of-Fit Criteria

Reflective and Formative Indicators

When analyzing latent variables and their relation, it is necessary to make them measurable by observable indicators (Edwards and Bagozzi 2000). Therefore, not only the goodness of the structural equation model has to be tested, but as well the quality of the measurement instruments. Only reliable measures allow statements on a structural level (e.g., Churchill 1979; Diamantopoulos and Winklhofer 2001; Edwards and Bagozzi 2000; MacKenzie et al. 2011). Latent variables are theorized and unobservable constructs that can only be approximated by measurable or observable indicators (e.g., Jarvis et al. 2004). Whereas, observed indicators are variables that are collected from respondents through several data gathering methods (Diamantopoulos and Winklhofer 2001; Edwards and Bagozzi 2000). The causality of the indicator and latent variable makes it necessary to distinguish between formative and reflective measures when operationalizing complex constructs (Diamantopoulos and Winklhofer 2001). In both cases, it is possible to have multiple indicators per latent variable for the operationalization. In reflective measurement models, the latent variable is causing the indicators (Edwards and Bagozzi 2000). This means that a change in the latent variable is causing changing values of all indicators, which leads to the expectation that all indicators are highly correlated (Diamantopoulos and Winklhofer 2001). When omitting a reflective indicator from a measurement model it incurs no negative consequences, however, the error rate of the measurement instrument might increase (Churchill 1979). In contrast, when a formative measurement model is developed, the indicators are causing the latent variable and therefore are not necessarily highly correlated. Hence, formative indicators cannot simply be omitted from the measurement model, all of them should be included. Otherwise, significant content of the construct might be disregarded (Coltman et al. 2008). However, because of the fact that formative indicators are not surely correlating it is not always possible to assess the goodness-of-fit of formative indicators. On the other hand, the measurement of reflective indicators can be assessed easily (Diamantopoulos and Winklhofer 2001). In the prevalent study, formative measures are not needed. In the present model, all constructs are measured with reflective indicators.

Mediating Effects

As the research model includes a potential mediating effect of *Trust into Employer* on the relationship of *Psychological Contract Breach* and *PIBV*, as well as *Psychological Contract Violation* and *PIBV*, this effect will be introduced and explained. Besides, it will be illustrated how this effect can be tested in science. In general, when testing for mediation it is investigated if the causal hypothesis that an independent construct (X) is causing a mediator (M), which in turn is causing a dependent construct (Y) (Figure 10) (Baron and Kenny 1986).

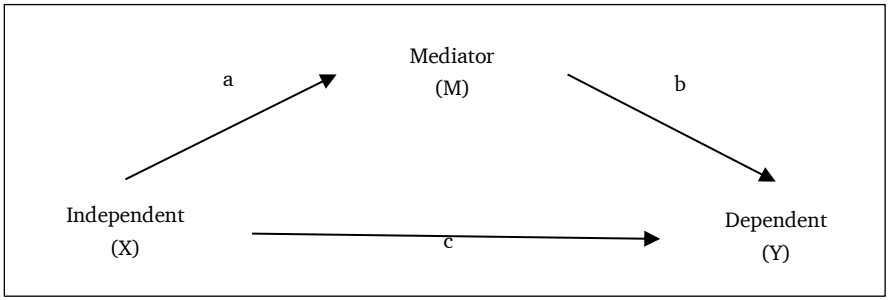


Figure 10: Exemplary Moderating Effect

As Zhao, Lynch Jr., and Chen (2010) describe, there are different types of mediation which have to be distinguished and identified during analysis. They distinguish among:

(1) Indirect-only mediation: ($a \times b$) is significant but (c) is not.
(2) Direct-only nonmediation: ($a \times b$) is not significant but (c) is.
(3) No effect nonmediation: *neither* ($a \times b$) nor (c) is significant.
(4) Competitive mediation: ($a \times b$) and (c) are significant.

When testing for mediation helps to model indirect effects efficiently, as they result through the multiplication of path coefficients. Preacher and Hayes (2004) recommend bootstrapping for computing mediating or nonmediating effects in structural equation modeling. Bootstrapping describes the computation of an indirect effect ($a \times b$) through random sampling of the overall sample. For each sample the indirect effect is calculated. Afterwards an empirical confidence interval is formed with the results. If the indirect effect ($a \times b$) could be computed in more than 95% of the samples, the mediating effect can be considered as evident (Zhao et al. 2010). These 95% define the confidence interval of the measured relation. The interval is indicating significance of a mediation if it does not include zero (Zhao et al. 2010).

Local Goodness-of-Fit

Different criteria can assess the local goodness-of-fit of the measurement of a latent variable with observable indicators. Generally, it is assumed that a specific value can be observed when measuring an indicator variable, for example by retrieving information on a Likert-Scale (e.g.,

Churchill 1979; DeVellis 2016). Nevertheless, in reality, it is unlikely that the observed value is equal to the real value of the latent construct (DeVellis 2016). The deviation between the observed and true value of a variable is caused by two different causes, which can be illustrated by the following equation (e.g., Churchill 1979; Herrmann et al. 2008).

$$x = t + s + e$$

Whereas x is the observed value of the variable and is composed of t, the 'true' value of the observed variable plus response errors s $(systematic\ error)$ and e $(random\ error)$. A measurement can be identified as valid, if the differences in the observed scores are reflecting real differences on the indicators which should be measured. This means that perfect validity is given, when $x = t$ without response errors (Churchill 1979). Further, the reliability of a measurement can be guaranteed if measures of the same construct, which are independent but comparable, are compatible (Churchill 1979). Thus, for a completely reliable measure the expected value of the random error e should be zero: $E(e) = 0$. Therefore, measure reliability is a necessary, but not sufficient condition for the validity of a measure (Churchill 1979).
For assessing the validity of measures it is common to distinguishing among four facets of validity (e.g., Homburg and Giering 1996; Venkatraman and Grant 1986). Namely, *content validity, convergent validity, discriminant validity* and *nomological validity*. *Content validity* is given when the measurement variables mirror a specific domain of content of the construct (MacKenzie et al. 2011; Venkatraman and Grant 1986). Thus, for ensuring content validity, it is important to have an explicit definition of the individual constructs (MacKenzie et al. 2011). Ensuring content validity is done in advance, during the scale and survey development, by expert reviews and the examination of the extent of consistency among their opinions (MacKenzie et al. 2011; Venkatraman and Grant 1986). *Convergent validity* refers to the characteristic of a construct measurement with multiple indicators that the indicators have a sufficiently strong relationship with each other. This means that the degree to which several attempts measuring the same construct with different methods are in agreement (Venkatraman and Grant 1986). The *discriminant validity* demands that indicators of various constructs are generating different measurement results. Hence, it explains the extent to which a construct is differing from another construct (e.g., Bagozzi and Phillips 1982; Venkatraman and Grant 1986). *Nomological validity* for a measure is given when the measured construct shows empirical relations to other constructs, which are demanded by a superordinate theoretical foundation. That means that it is describing the degree to which predictions from this theoretical foundation are verified by the measure (Venkatraman and Grant 1986).

Empirical research uses several local goodness-of-fit measures to assess the reliability, convergence, as well as the discriminant validity of construct measurements. In the following, important and relevant goodness-of-fit measures for indicator and factor reliability as well as validity are presented.

As a standard measure, *Cronbach's Alpha* is used to assess the reliability of the indicator variables of a construct (e.g., Gefen et al. 2000; MacKenzie et al. 2011). All indicators are combined in

every possible combination and divided into two parts. Respectively the correlation of the sum of the one-half of the variables with the sum of the other half of the variables is determined. Afterwards, the mean of the estimated correlations is calculated. The value range of Cronbach's Alpha is between 0 and 1, whereas higher values are representing increased reliability among indicators (Threshold of ≥ 0.7) (Gefen et al. 2000; MacKenzie et al. 2011). The following equation formally describes the evaluation of Cronbach's Alpha, with m as number of items, $\overline{Cov}$ as average covariance of items, and $\overline{Var}$ as average variance of items:

$$\alpha = \frac{m \cdot \overline{Cov}}{(\overline{Var} + (m-1)\overline{Cov})}$$

Since Cronbach's Alpha does not provide any diagnostic information at the indicator level of a construct, the *Item-to-Total correlation* is used to calculate the correlation between indicators. It is defined as the correlation of an indicator to the sum of the indicators of the construct (Homburg and Giering 1996). If Cronbach's Alpha is too low, the Item-to-Total correlation can identify the indicator, which has the lowest correlation with the other indicators. To strengthen the empirical meaning of the latent variable, this indicator should be excluded from the measurement (Jarvis et al. 2004).

The *Indicator Reliability (IR)* specifies the share of the variance of an indicator that is explained by the underlying construct (Homburg and Giering 1996). The following equation shows the formal calculation (e.g., Herrmann et al. 2008):

$$IR(x_i) = \frac{\lambda_{ij}^2 \Phi_{jj}}{\lambda_{ij}^2 \Phi_{jj} + \theta_{ii}}$$

The term λ_{ij} is the estimated factor loading of the indicator x_i, Φ_{jj} is the estimated variance of the factor, and θ_{ii} is the estimated variance of the measurement error (Schäffer 2007). For the IR no hard threshold values exist, but typically indicator reliabilities ≥ 0.4 are considered as good (IR can have values between 0 and 1) (Brown 2015).

To measure the convergent validity of a construct it is typical to examine the *Construct Reliability (CR)* as well as the *Average Variance Extracted (AVE)* of a factor (e.g., MacKenzie et al. 2011). Both goodness-of-fit measures show how good a construct can be measured by all its related indicators (Brown 2015). The measures can take values between 0 and 1, with small values indicating insufficient convergent validity of the construct (Herrmann et al. 2008; MacKenzie et al. 2011). The following two formulas are illustrating the estimation (Herrmann et al. 2008):

$$CR\left(\xi_j\right) = \frac{(\sum_{i=1}^{k} \lambda_{ij})^2 \Phi_{jj}}{(\sum_{i=1}^{k} \lambda_{ij})^2 \Phi_{jj} + \sum_{i=1}^{k} \theta_{ii}}$$

$$AVE\left(\xi_j\right) = \frac{\sum_{i=1}^{k} \lambda_{ij}^2 \Phi_{jj}}{\sum_{i=1}^{k} \lambda_{ij}^2 \Phi_{jj} + \sum_{i=1}^{k} \theta_{ii}}$$

The recommended threshold for construct reliability is 0.7 and 0.5 for the average variance (MacKenzie et al. 2011).

Additionally, the assessment of the discriminant validity of the measured variables is necessary. Therefore, the application of the *Fornell-Larcker-Criterion* (FLC) has become established in economic research (MacKenzie et al. 2011). The criterion is satisfied when the squared correlation between two constructs is higher than the AVE of the individual constructs. This means that each latent variable explains a greater proportion of variance of its own indicators than it is sharing with other constructs (MacKenzie et al. 2011).

In summary, the following table (Table 16) illustrates the local goodness-of-fit measures on construct and indicator level.

Name	Threshold
Cronbach's Alpha	≥ 0.7
Indicator Reliability (IR)	≥ 0.4
Construct Reliability (CR)	≥ 0.7
Average Variance Extracted (AVE)	≥ 0.5
Fornell-Larcker-Criterion (FLC)	AVE ≥ Square correlation of other constructs in the model

Table 16: Overview of Local Goodness-of-Fit Measures

Potential sources of systematic survey errors

A further challenge when collecting data by conducting socio-scientific research is the handling of systematic survey errors, as the Common Method Bias (CMB), the Key Informant Bias, the Social Desirability Bias and response patterns. The CMB describes the distortion of the sample's covariance structure caused by the fact that the same data source was used for measuring all variables, dependent and independent, in a certain dependency analysis model (Homburg and Klarmann 2006; MacKenzie et al. 2011). For example, when conducting data collection with surveys it is possible that similar formulations or the context of the data collection might have an impact on the response behavior and therefore might cause a systematic measurement error (e.g., Podsakoff et al. 2003; Podsakoff, MacKenzie, and Podsakoff 2012). The Key Informant Bias can arise when the data collection has taken place through key informants that might have information differences (e.g., Phillips 1981). Additionally, the Social Desirability Bias is describing the potential distortion of the sample's covariance structure by the fact that respondents have the tendency to answer in a way that is viewed favorably by others (e.g., Fisher 1993). Another bias can be caused by the fact that respondents tend to favor certain answer categories, like the tendency to agree or the tendency to use middle-points (Podsakoff et al. 2012).

To prevent these biases, several things can be considered in advance. For example, it is recommended to use various survey methods and for example different survey subjects or points in time to conduct the survey (Podsakoff et al. 2003, 2012). Additionally, it is recommended to avoid wording that increases the impression that people should answer as socially desired or that increases response patterns, as for example the word *'all'* in a statements or question usually produces overstatement ('The product meets *all* my expectations') (Churchill and Iacobucci 2005). To assure low systematic biases, it is also important to assure the respondents that their answers are treated anonymously, that there are no wrong and right answers and that they should respond to the questions spontaneously without rethinking the questions too often (Podsakoff et al. 2003). With the help of statistical methods, a methodological bias can also be examined after the data collection. Therefore, several approaches can be applied. As for example, the Harman's single-factor test, which is conducted by loading all variables of the model into an exploratory factor analysis. The unrotated factor solutions are inspected to control for the amount of factors, necessary to account for the variance in the variables (Podsakoff et al. 2003). A significant extent of common method variance is existing when one factor materializes from the factor analysis or if a general factor is responsible for the majority of the covariance between the measures. Another recognized method is to add an unmeasured latent variable to the research model, which is uncorrelated with the variables of the model and on which all measured indicators can load (Podsakoff et al. 2003). By adding the latent variable, it is possible to exclude the joint variance of all observed variables from the model (Podsakoff et al. 2012). If the factor loading of the indicators' substantive variances are substantially greater than the variance of the common latent factor loadings, it can be concluded that no CMB is existing (Schäffer 2007). Furthermore, the squared values of the latent common factor loadings can be understood as the percentage of item variance caused by the survey method, whereas the squared values of the existing constructs can be interpreted as the percentage of item variance caused by the construct itself (Liang et al. 2014).

5.6.2. Operationalization and Validation of Constructs

Most of the constructs in this study (i.e., *Psychological Contract Breach* and *Violation, Trust into Employer, Perceived Control, Sensitivity of Information, Perceived Benefits,* and *Intention to Disclose*) have been well established in the existing literature. Therefore, previously validated measures can be applied and adapted as appropriate. All adapted items were modified, based on the validation procedures described in the literature of MacKenzie et al. (2011) and followed the established instruction on wording questions when developing and confirming a questionnaire by (De Vaus 2002). To ensure content validity, subject matter experts reviewed the survey. The questionnaire was piloted among 16 employees (serving as experts) of a large company in Europe before being accepted as the final version. There was no necessity to drop items from the test. Appendix A lists all measurement items and related sources of the survey. According to the fact that there was no reliable scientific source for scales of the items of the self-developed constructs *PIBV* and *Resistance*, they had to be carefully developed following the approach by MacKenzie et al. (2011). The measures for PIBV were accurately and thoroughly

derived. While Dinev and Hart (2004) measured the perceived vulnerability of users of the internet in general, a seven-item scale was developed to measure PIBV by capturing the employee's perception of information-based vulnerability when using REIS (see Table 17).

Perceived Information-Based Vulnerability (PIBV) captures a user's perceptions that information entered into a system can be used in an opportunistic manner by the employer.	
PIBV 1	Submitted information could be misused.
PIBV 2	Submitted information could be made available to unknown individuals in my company without my knowledge.
PIBV 3	Submitted information could be inappropriately used.
PIBV 4	Submitted information could be used to my disadvantage.
PIBV 5	It might be beneficial for my company to use submitted information without considering my interests.
PIBV 6	Submitted information could be used for unfavorable personal decisions.
PIBV 7	Submitted information could be exploited by the company.

Table 17: Measurement Items of *Perceived Information-Based Vulnerability*

To ensure *content validity* of the items and thus the representativeness of the objects regarding an aspect of the content domain of the construct, the formerly collected interviews (see Section 4) built the foundation of the item development for PIBV. Additionally, to correspond to the conceptualization and thus ensure *construct validity*, the items were carefully worded to refer to the employee's perception of possible vulnerability when disclosing personal information by the employer, rather than being general and referring to any software system within the company.

Apathy can be labeled as a neutral or transition zone of resistance, characterized by a lack of positive or negative emotions or attitudes.	
AP 1	I feel indifferent towards the system
AP 2	I don't care about the system
AP 3	I am not interested in the system
Passive resistance exists when mild or weak forms of disagreement are encountered, and negative perceptions or attitudes towards a system are existent.	
PR 1	I perceive the system as a negative change
PR 2	I have a negative attitude towards the system
PR 3	I would like to distance myself from the system
Active resistance is typified by strong but not destructive opposing behavior such as blocking or impeding the system.	
AR 1	I would ask others not to use the system
AR 2	I would reject the system
AR 3	I would point out my negative view regarding the system to others

Table 18: Measurement Items of the Resistance Constructs

The measurement items for the construct *Resistance* has been developed based on the recommendation of Lapointe and Rivard (2005) to divide resistance into sub-levels – namely *Apathy*, *Passive Resistance*, *Active Resistance*, and *Aggressive Resistance* (see Table 18). *Aggressive Resistance* was dropped from the scale during the scale development process and review sessions with experts, as it reflects destructive behavior such as purposeful destruction, spoilage, or even terrorism. Those behaviors were found to be too strong by experts. Domain experts pointed out that no employee would react with terroristic behavior just because of a software solution. In the following, the process of scale development and refinement of *PIBV* and *Resistance* will be described in detail. Table 18 and 19 serve as matching tables for abbreviations of final PIBV and Resistance items.

Scale Development and Content Adequacy

In the first step, a first draft of the items was developed for doing further refinements and adequacy checks (see Table 19). As Table 17 and 18 serve as matching tables for the final version of the self-developed items, Table 19 serves as a matching table for the first draft of the items.

PIBV (1st draft)	
PIBV 1-D	Information submitted in the system could be misused.
PIBV 2-D	Information submitted in the system could be made available to unknown individuals in my company without my knowledge.
PIBV 3-D	Information submitted in the system could be inappropriately used.
PIBV 4-D	Information submitted in the system could be used to my disadvantage.
PIBV 5-D	It might be beneficial for my company to use information submitted in the system without considering my interests.
PIBV 6-D	Information submitted in the system could be used for unfavorable personal decisions.
PIBV 7-D	Information submitted in the system could be exploited by the company.
Apathy (1st draft)	
AP 1-D	I feel indifferent towards the system
AP 2-D	I would like to distance myself from the system
AP 3-D	I am not interested into the system
Passive Resistance (1st draft)	
PR 1-D	I would find excuses not to use the system
PR 2-D	I would not use the system
PR 3-D	I would withdraw the system
Active Resistance (1st draft)	
AR 1-D	I would ask others to form coalitions against the system
AR 2-D	I would point out opposite views regarding the system to others
AR 3-D	I would ask others to intervene against the system

Table 19: First Draft of Self-Developed Measurement Items

For this first version, the *content adequacy* had to be tested. Therefore, a recommended method by MacKenzie et al. (2011) was applied. A matrix has been constructed, in which the definitions of items of PIBV and items of the construct Resistance were listed at the top of the columns and the developed items were listed in the rows. Raters were asked to decide on the degree to which an item was capturing the constructs, by using a five-point Likert-type scale (1=not at all – 5=completely). After the first round of measurement (n=16), a one-way repeated measure ANOVA was used to assess if one of the item's mean rating on an aspect of the construct's domain differed from the ratings on the other dimensions of the construct's domain (MacKenzie et al. 2011).

	f-Statistic	**p-Value (≤ 0.05)**
PIBV 1-D	23.45	$1.3*10^{-12}$
PIBV 2-D	15.59	$2.5*10^{-9}$
PIBV 3-D	27.8	$3.6*10^{-14}$
PIBV 4-D	16.63	$8.5*10^{-10}$
PIBV 5-D	16.27	$1.2*10^{-9}$
PIBV 6-D	28.17	$2.7*10^{-14}$
PIBV 7-D	36.73	$5.5*10^{-17}$
AP 1-D	129.9	$3.3*10^{-26}$
AP 2-D	7.24	$3.2*10^{-4}$
AP 3-D	46.35	$1.3*10^{-15}$
PR 1-D	8.32	$1.0*10^{-4}$
PR 2-D	10.14	$1.7*10^{-5}$
PR 3-D	12.37	$2.1*10^{-6}$
AR 1-D	31.42	$2.5*10^{-12}$
AR 2-D	16.42	$6.6*10^{-8}$
AR 3-D	17.67	$2.5*10^{-8}$

Table 20: ANOVA Test Results of Self-Developed Measurement Items

Since in all measures, the f-statistics were significant or at least the p-values were smaller than alpha (0.05) (see Table 20), a planned contrast was conducted to analyze if the mean rating for the item on the hypothesized aspect of the construct domain was higher than the mean of the rating for this item on all other aspects of the construct domain.

	Perceived Information-Based Vulnerability	Apathy	Passive Resistance	Active Resistance
PIBV 1-D	4.79	1.57	2.36	1.29
PIBV 2-D	4.43	1.43	2.14	1.57
PIBV 3-D	4.64	1.64	2.14	1.64
PIBV 4-D	4.86	1.43	2.21	1.71
PIBV 5-D	4.07	2.21	2.21	1.86
PIBV 6-D	4.64	1.50	2.14	1.64
PIBV 7-D	4.71	1.57	2.14	1.50

Table 21: Planned Contrast for *Perceived Information-Based Vulnerability*

After the planned contrast test, it could be concluded that the items of the construct PIBV met the item validity criteria and could be retained (Table 21). Several items of the resistance constructs had been revised, adapted and redefined (see Table 22).

Apathy (2nd draft)	
AP 1-D2	I feel indifferent towards the system
AP 2-D2	I don't care about the system
AP 3-D2	I am not interested in the system
Passive Resistance (2nd draft)	
PR 1-D2	I have a negative attitude towards the system
PR 2-D2	I would like to distance myself from the system
PR 3-D2	I perceive the system as a negative change
Active Resistance (2nd draft)	
AR 1-D2	I would point out my negative view regarding the system to others
AR 2-D2	I would ask others not to use the system
AR 3-D2	I would reject the system

Table 22: Second Draft of Measurement Items of Resistance Constructs

To test the second draft of measurement items of the resistance constructs concerning item validity, the same procedure was applied. The one-way ANOVA test, as well as the following planned contrast with a new sample indicated that no changes had to be made to achieve adequate item validity (see Table 23).

	Apathy	Passive Resistance	Active Resistance
AP 1-D2	5	2	1.43
AP 2-D2	4.86	1.86	1.28
AP 3-D2	4.85	1.43	1.14
PR 1-D2	1.28	4	3.4
PR 2-D2	2	3.8	2.6
PR 3-D2	1.43	4	3
AR 1-D2	1	2.43	4
AR 2-D2	1.14	1.85	4.7
AR 3-D2	1	2.14	4.29

Table 23: Planned Contrast for Resistance Constructs

Scale Evaluation and Refinement

PIBV	
PIBV 1	Submitted information could be misused.
PIBV 2	Submitted information could be made available to unknown individuals in my company without my knowledge.
PIBV 3	Submitted information could be inappropriately used.
PIBV 4	Submitted information could be used to my disadvantage.
PIBV 5	It might be beneficial for my company to use submitted information without considering my interests.
PIBV 6	Submitted information could be used for unfavorable personal decisions.
PIBV 7	Submitted information could be exploited by the company.
Apathy	
AP 1	I feel indifferent towards the system.
AP 2	I don't care about the system.
AP 3	I am not interested in the system.
Passive Resistance	
PR 1	I disagree with the implementation of the system.
PR 2	I perceive the system as a negative change.
PR 3	I have a negative attitude towards the system.
Active Resistance	
AR 1	I will ask others to not use the system.
AR 2	I will reject the system.
AR 3	I will point out my negative view regarding the system to others.

Table 24: Final Version of Self-Developed Items

To measure the construct *PIBV* of REIS users and *Resistance* against the system, new scales were developed in advance of the data collection. In a pre-test, all indicators were tested regarding

their comprehensibility. The pre-tests were performed by sending out an online survey to a specific target group of 200 (n=76) employees of one company. The group was asked to do the survey and give feedback, in a comment field, about unclear statements and the survey in general. This approach allowed to test for possible misunderstandings and unclear or ambiguous formulations of items and again helped to ensure the content validity of the self-developed measures. Afterwards, further sharpening of the wording of the items was done (Table 24).

In the first step, a correlation matrix was developed to test the correlation among all items. The correlation helps to omit items measuring the same (high correlation coefficient ≥ 0.8) (De Vaus 2002, p. 116). This procedure was used to omit items of PIBV for the structural equation model. As shown in Table 25 *PIBV4* and *PIBV6* were omitted, as they had a high correlation coefficient with other items of the construct (*PIBV6* with *PIBV7* and *PIBV4* with *PIBV3*). After the exclusion the correlations were adequate and for the final structural equation model five PIBV items were included.

	PIBV 1	PIBV 2	PIBV 3	PIBV 4	PIBV 5	PIBV 6	PIBV 7
PIBV 1	1.00						
PIBV 2	0.74	1.00					
PIBV 3	0.80	0.81	1.00				
PIBV 4	0.77	0.72	**0.82**	1.00			
PIBV 5	0.59	0.49	0.60	0.64	1.00		
PIBV 6	0.66	0.60	0.69	0.77	0.67	1.00	
PIBV 7	0.71	0.64	0.73	0.79	0.73	**0.86**	1.00

Table 25: Correlation Matrix for *Perceived Information-Based Vulnerability*

Furthermore, all self-developed items were tested regarding their validity and reliability. In the following, the local goodness-of-fit of the measurement model on construct and item level of PIBV is discussed.

Perceived Information-Based Vulnerability – PIBV			
Items 7-point Likert-Scale (1=strongly disagree - 7=strongly agree)		**Item-to-Total Correlation**	**Indicator Reliability**
Quality Criteria on Item Level			
PIBV 1	Submitted information could be misused.	0.89	0.76
PIBV 2	Submitted information could be made available to unknown individuals in my company without my knowledge.	0.85	0.71
PIBV 3	Submitted information could be inappropriately used.	0.91	0.85
PIBV 5	It might be beneficial for my company to use submitted information without considering my interests.	0.79	0.47
PIBV 7	Submitted information could be exploited by the company.	0.88	0.66
Quality Criteria on Construct Level			
Cronbach's Alpha		0.91	
Construct Reliability		0.92	
Average Variance Extracted		0.69	
Fornell-Larcker-Criterion		Fulfilled	

Table 26: Local Goodness-of-Fit of *Perceived Information-Based Vulnerability*

Table 26 illustrates the measurement of the Construct *PIBV*. All prerequisites regarding measurement quality on construct and item level are met. Therefore, the measurement of the construct is expected to be valid.

Apathy			
Items 7-point Likert-Scale (1=strongly disagree - 7=strongly agree)		**Item-to-Total Correlation**	**Indicator Reliability**
Quality Criteria on Item Level			
AP 1	I feel indifferent towards the system	0.84	0.57
AP 2	I don't care about the system	0.89	0.82
AP 3	I am not interested in the system	0.83	0.46
Quality Criteria on Construct Level			
Cronbach's Alpha		0.82	
Construct Reliability		0.83	
Average Variance Extracted		0.62	
Fornell-Larcker-Criterion		Fulfilled	

Table 27: Local Goodness-of-Fit of *Apathy*

The measurement values of the construct *Apathy* do not show any problematic measurement. Table 27 indicates that the measured values exceed the recommended thresholds both on the indicator and on the construct level.

Passive Resistance			
Items 7-point Likert-Scale (1=strongly disagree - 7=strongly agree)		**Item-to-Total Correlation**	**Indicator Reliability**
Quality Criteria on Item Level			
PR 1	I disagree with the implementation of the system.	0.94	0.81
PR 2	I perceive the system as a negative change.	0.96	0.89
PR 3	I have a negative attitude towards the system.	0.96	0.89
Quality Criteria on Construct Level			
Cronbach's Alpha		0.95	
Construct Reliability		0.95	
Average Variance Extracted		0.87	
Fornell-Larcker-Criterion		Fulfilled	

Table 28: Local Goodness-of-Fit of *Passive Resistance*

Table 28 shows the measuring instrument of *Passive Resistance*. With regard to this measurement instrument, it can also be assumed that the scale adequately satisfies all requirements for the measurement quality.

Active Resistance			
Items 7-point Likert-Scale (1=strongly disagree - 7=strongly agree)		**Item-to-Total Correlation**	**Indicator Reliability**
Quality Criteria on Item Level			
AR 1	I will ask others to not use the system.	0.83	0.54
AR 2	I will reject the system.	0.97	0.86
AR 3	I will point out my negative view regarding the system to others.	0.97	0.61
Quality Criteria on Construct Level			
Cronbach's Alpha		0.92	
Construct Reliability		0.86	
Average Variance Extracted		0.67	
Fornell-Larcker-Criterion		Fulfilled	

Table 29: Local Goodness-of-Fit of *Active Resistance*

Finally, the measurement of *Active Resistance* against REIS was assessed with regard to its quality. As it can be seen in Table 29, all key factors exceed the required thresholds. Overall, a good quality of the measuring instrument is to be assumed.

5.6.3. Survey Design and Data Collection Process

To test the research model, the survey method was chosen. This method helps to gain insights on personal and social facts, attitudes and beliefs of people in a generalizable way. Since this quantitative approach enjoys the merit of enhancing the generalizability of research findings (Fang et al. 2014) it perfectly fits the goal of this subsection to find a generalizable model for the sensitive information disclosure behavior of employees when using enterprise software solutions and their perceived information-based vulnerability. For the collection of survey results, an electronic survey method was chosen. The tool used was a survey tool provided by the evaluated company.

The recruitment of participants of the test study happened in a globally acting company with headquarter in Europe and employing more than 10.000 people. After an agreement with the works council of the company, 3.000 random people of the workforce were invited to answer the survey. The response rate was 10.9% (327 People), of those 25% were female and 75% male. 22% of the respondents were between 20 and 29 years old, 26% between 30 and 39 years old, 31% between 40 and 49, 21% older than 50. On average 53% have been employed at that company for more than ten years, 13% have been with the company for more than five but less than ten years, and 35% less than five years.

Since PIBV is a system characteristic and therefore referring to the (planned) usage of a specific REIS, the test of the model was linked to a fictitious implementation of a representative REIS system. Participants were invited to watch a user video (showing the functionality of the solution, as well as a list of information that could be inserted into the system) and a description of the system to get a common understanding of the tool that should be evaluated. In the following, the provided description of the software solution, called 'People Involvement' (also fictitious name) is given:

> *'Do you know that too? You participate in an employee survey and feel that you cannot achieve anything and that nothing changes? With this software solution 'People Involvement' you can confidently provide feedback on your work satisfaction at any time. Based on your needs you receive specially tailored actions to improve your satisfaction. Start with your personal profile and select your critical needs out of a catalog, developed by experts. Evaluate your current satisfaction and comment on the reason for your current satisfaction with your individual needs. Don't worry; you are the only one who has access to your personal profile. For other people in the company, your information is only available as aggregate.*
>
> *Based on your created profile the system recommends possible actions to improve your satisfaction. You can customize proposed measures to suit them to your individual needs. Now you can discuss the options with your manager. To have control over your actions, it is no problem to cancel your actions at any point in time.*
>
> *To support you, your manager has access to your proposed actions as well as the proposal of actions of your whole team. He can thereby draw your attention to appropriate*

measures, which best improve your job satisfaction. In your information area, you can find interesting and useful evaluations, about yourself, your team or the whole company in real time.

You and your manager have access to statistics and information about the aggregated actual satisfaction, the satisfaction over time, running actions, anonymous information about comments (Tag Cloud) and the actual needs of the workforce. All statistics can be shown on personal, team, organizational and company level. Nevertheless, for aggregated data, there have to be more than 9 data points to ensure data security.'

All participants received an invitation by e-mail, which contained a short introductory section to the survey, additional information about the software system, to be evaluated, and a link to the questionnaire. The introductory section contained information about the approximate duration of the questionnaire (12 minutes), the information that data collection and analysis will be anonymous, and that it will not be possible to draw conclusions about the participants. Just to be sure that all respondents had the same understanding of the software system the introductory video and introductory text had been added. The participants had the possibility to gather further information about the system's functionality, purpose, data security and privacy concept. All information provided in the e-mail were distributed to prevent systematic errors, such as a Common Method or Key Informant Bias.

5.7. Results of the Data Analysis

In this section, the results of the model testing are illustrated and discussed for further model specification and development. The respective R code can be found in Appendix B.[7]

5.7.1. Assessment of Local Goodness-of-Fit

In the course of the described validation study, the confirmed scales could now be used for the evaluation of the latent variables (see subsection 5.6.2). Table 30 again illustrates the results of the identified goodness-of-fit values of the data, interrogated by this primary study (see Section 5.6.1).

Construct	Cronbach's Alpha	CR	AVE	FLC
PIBV	0.91	0.92	0.69	Fulfilled
Apathy	0.82	0.83	0.62	Fulfilled
Passive Resistance	0.95	0.95	0.87	Fulfilled
Active Resistance	0.92	0.86	0.67	Fulfilled

Table 30: Local Goodness-of-Fit of Measurement Model

All requirements, as described in subsection 5.6.1, that the construct PIBV and the Resistance constructs should achieve, were met (see Table 30). The Cronbach's Alpha and the Construct

[7] To protect the employees, due to regulations of the company and privacy concerns of the works council the collected raw data will not be published.

Reliability (CR) were higher than the threshold of 0.7, and the Average Variance Extracted (AVE) was greater than the threshold of 0.5. Furthermore, the Fornell-Larcker-Criterion was fulfilled, as each square of the correlation of the items of PIBV and the Resistance constructs were lower than the AVE (see Appendix C for the results of the test).

5.7.2. Descriptive Statistics and Correlation Analysis

To interpret the collected data, a descriptive analysis of the response behavior was conducted. The mean and standard deviation of each construct are of particular interest.[8] By computing the average of a latent variable as a standard measure of a statistical distribution, the answer to a specific question of an average respondent of the sample can be shown (e.g., De Vaus 2014). The standard deviation is used to interpret the scatter of a variable, and it illustrates the heterogeneity (high scatter) or homogeneity (slight scatter) of the response behavior regarding a variable (e.g., De Vaus 2014).

Construct	Mean	Standard Deviation
Sensitivity of Information	4.32	1.79
Perceived Control	3.54	1.75
Psychological Contract Breach	2.61	1.53
Psychological Contract Violation	1.56	1.17
Trust into Employer	5.24	1.46
PIBV	4.91	1.55
Perceived Benefits	4.55	1.54
Intention to Disclose	4.01	1.76
Apathy	3.42	1.62
Passive Resistance	3.33	1.76
Active Resistance	2.71	1.75

Table 31: Mean and Standard Deviation of Latent Variables

As already mentioned in Section 5.6.2 all manifest variables were measured with a 7-point Likert-Scale. Table 31 illustrates that all values are varying between 1.56 and 5.24. A relatively low mean value of *Psychological Contract Breach* and the even lower mean of *Psychological Contract Violation* could be identified. This indicates that participants rated the breach, as well as the violation of the psychological contract as rather low. Contrary to that, employees rated their trust into the employer with a rather high average value of 5.24. The descriptive statistic indicates that employees tended to answer questions on their employer-employee relationship in a more positive way with a high trust relationship and a low level of psychological contract breaches and violations. Furthermore, the *PIBV* and *Perceived Benefits* of employees reached a similar mean, whereas the average of the former was slightly higher. Employees perceive

[8] Since each latent variable was measured by several reflective indicators, the mean for each latent variable was calculated by computing the average value of the indicators.

potential vulnerability from disclosing in the system, but at the same time see benefits from the publication of information in REIS.

To get a feeling for the relationship between the latent variables, a bivariate correlation analysis between constructs was conducted. The analysis describes the shared variation of latent variables and has the purpose of determining the empirical relation among them (Babbie 2010). The interpretation of the correlation is consolidated by analyzing the correlation coefficient, which is illustrating the strength of a direct relationship between two variables (e.g., Chatterjee and Hadi 2015). The correlation coefficient has a range from [-1, 1], where a negative value is interpreted as a negative direct relationship among the constructs and vice versa. If a value is close to 0, there is no direct relationship existing between the two variables (De Vaus 2014). Table 32 illustrates the pairwise correlation coefficients of all latent variables of the model.

Constructs		1	2	3	4	5	6	7	8	9	10	11
1	Sensitivity of Information	1.00										
2	Perceived Control	-0.40	1.00									
3	Psych. Contract Breach	0.12	-0.24	1.00								
4	Psych. Contract Violation	0.08	-0.16	0.66	1.00							
5	Trust into Employer	-0.08	0.16	-0.68	-0.61	1.00						
6	PIBV	0.50	-0.51	0.22	0.22	-0.25	1.00					
7	Perceived Benefits	-0.42	0.55	-0.15	-0.1	0.10	-0.36	1.00				
8	Intention to Disclosure	-0.38	0.47	-0.14	-0.1	0.11	-0.42	0.75	1.00			
9	Apathy	0.11	-0.13	0.04	0.03	-0.03	0.10	-0.23	-0.15	1.00		
10	Passive Resistance	0.40	-0.47	0.15	0.12	-0.13	0.50	-0.69	-0.76	0.21	1.00	
11	Active Resistance	0.37	-0.45	0.14	0.11	-0.12	0.47	-0.65	-0.75	0.14	0.92	1.00

Table 32: Correlation Matrix of all Latent Variables

A particularly significant relation could be found between *Perceived Benefits* and *Intention to Disclose* (correlation coefficient = 0.75). A similar correlation was found between *Passive Resistance* (-0.76) and *Active Resistance* (-0.75) with *Intention to Disclose*. This indicates a direct negative relation between disclosure intention and resistance against REIS. Moreover, *Perceived Benefits* seem to have a significant relation with *Passive Resistance* (-0.69) and *Active Resistance* (-0.65). Especially strong negative correlations could also be identified among the variables *Psychological Contract Breach* (-0.68) and *Psychological Contract Violation* (-0.61) with *Trust into Employer*. A similar correlation could be found between *Psychological Contract Breach* and *Violation* (0.66). This relationship confirms the findings from the Psychological Contract Theory (Robinson and Morrison 2000). Furthermore, significant correlations were found between

Perceived Sensitivity of Information and *PIBV* (0.54), as well as *Perceived Control* and *PIBV* (-0.52). It appears that the insights from Privacy Calculus Theory that the sensitivity of information has a high impact on the concerns of people (e.g., Bansal et al. 2010; Yang and Wang 2009) also holds true for the perception of PIBV. The matrix also indicates that the calculus of costs and benefits can be confirmed for the organizational context. *PIBV* plays an important role for disclosure in REIS (-0.42). Furthermore, the aspect of control plays a crucial role for people when perceiving vulnerability through information disclosure. The correlation matrix indicates a slight correlation between *Psychological Contract Breach* or *Psychological Contract Violation* and *PIBV* (both 0.22).

5.7.3. Assessment of Global Goodness-of-Fit

The introduced causal model in Section 5.4 and 5.5 was finally tested and analyzed with the statistic software R (version 3.3.2). The goal of the analysis was to test if the empirically identified covariance corresponds with the hypothesized model. However, before testing the hypotheses, an analysis of the global goodness-of-fit on the structural level was conducted (see Section 5.6.2). Thereby a χ^2-value of 0.00 with a degree of freedom of 832 was determined. Furthermore, the RMSEA was 0.06 and the calculated SRMR 0.09. The NNFI achieved a value of 0.90 and the CFI of 0.91. All values indicate an acceptable fit of the model regarding the determined covariance matrix.

For testing, a potential Common Method Bias, subsequently two test were applied. First the Harman's one-factor test (conducted with the tool SPSS), which resulted in a cumulated declared variance of 30%. Thus, 30% of the variance can be explained by a single factor. This indicates that the data set does not suffer from a common method bias issue because the variance explained by a single factor is less than 50%. To further clarify the non-existence of a CMB a Common Latent Factor (CLF) test was conducted. Therefore, a further latent variable was added to the model. This variable helps to control a possible bias that could be caused by the chosen survey method. As recommended by Podsakoff et al. 2003 all measured items from all constructs were included into this one latent variable to determine if the majority of variance can be explained by a single overall variable. To estimate the modified model, the correlation of the latent variable with all other latent variables of the model was inhibited. As illustrated in Appendix D, the results show that the average substantively explained variance of the items is 0.79, while the average common latent factor variance is 0.16. The ratio of substantive variance to the common latent factor variance is about 5:1. Given the magnitude of 5:1 of the CLF analysis and the result of the Harman's single-factor test, it can be concluded that a CMB is unlikely to be a serious concern for this study.

5.7.4. Hypotheses Testing

As all requirements of the local and global goodness-of-fit were fulfilled, the interpretation of the data analysis with regard to the hypothesized relations followed. Table 33 and Figure 11 show the results of the hypotheses analysis. The considerations that the perception of information-based vulnerability is decreasing the disclosure intention in REIS (H6-1) could be

confirmed with a negative effect (-0.19; p<0.001). With respect to PIBV, the relation with resistance levels could be partially confirmed. Hypothesis H6-2, reflecting the effect of *PIBV* on *Apathy*, was rejected due to insignificance (p>0.05). Nevertheless, H6-3 and H6-4 were found to be highly significant. This reflects the positive relation between *PIBV* and *Passive Resistance* (-0.36; p<0.001), as well as *Active Resistance* (-0.22; p<0.001). In addition to *PIBV*, the effect of *Perceived Benefits* on the possible outcomes was examined. It was found that *Perceived Benefits* have a highly significant positive impact on the *Intention to Disclose* information in REIS (H7-1) (0.76; p<0.001) and a strong significant negative effect on all resistance levels (H7-2, H7-3, H7-4).

H#	Effect	Path coefficient	Significance Level [a]	Result
1-1	Psychological Contract Violation on PIBV	0.12	n.s.	Not Confirmed
1-2	Psychological Contract Violation on PIBV, mediated through Trust into Employer	-0.32	0.022 CI [0.02 – 0.26]	Confirmed
2-0	Psychological Contract Breach on Psychological Contract Violation	0.46	0.000	Confirmed
2-1	Psychological Contract Breach on PIBV	-0.08	n.s.	Not Confirmed
2-2	Psychological Contract Breach on PIBV, mediated through Trust into Employer	-0.41	0.023 CI [0.02 - 0.21]	Confirmed
3	Trust into Employer on PIBV	-0.20	0.025	Confirmed
4	Sensitivity of Information on PIBV	0.41	0.000	Confirmed
5	Perceived Control on PIBV	-0.28	0.000	Confirmed
6-1	PIBV on Intention to Disclose	-0.19	0.000	Confirmed
6-2	PIBV on Apathy	0.03	n.s.	Not Confirmed
6-3	PIBV on Passive Resistance	0.35	0.000	Confirmed
6-4	PIBV on Active Resistance	0.22	0.000	Confirmed
7-1	Perceived Benefits on Intention to Disclose	0.76	0.000	Confirmed
7-2	Perceived Benefits on Apathy	-0.21	0.000	Confirmed
7-3	Perceived Benefits on Passive Resistance	-0.73	0.000	Confirmed
7-4	Perceived Benefits on Active Resistance	-0.45	0.000	Confirmed

Table 33: Results of Hypotheses Evaluation

[a]: CI = Confidence Interval of Bootstrap Analysis

Moreover, it could be shown that factors stemming from the employer-employee relationship and system characteristics influence PIBV. Whereas the system characteristics – *Sensitivity of Information* and *Control* of information submitted in the system – had an impact with high significance. Hypotheses H4 (0.4; p<0.001) and 5 could be affirmed (-0.28; p<0.001). With regard to employer-employee relationship factors, it could be confirmed that *'Trust in the Employer'* has a significant effect on *PIBV* (-0.2; p<0.05). However, the proposed direct effects

between *Psychological Contract Violation* and *PIBV* (H1-1), as well as *Psychological Contract Breach* and *PIBV* (H2-1) were found to be insignificant (p>0.1). Nevertheless, *Trust into Employer* was found to fully mediate *Psychological Contract Breach* and *PIBV*, as well as *Psychological Contract Violation* and *PIBV*. The mediating effect was tested in a bootstrap analysis, where the relations were found to be significant.

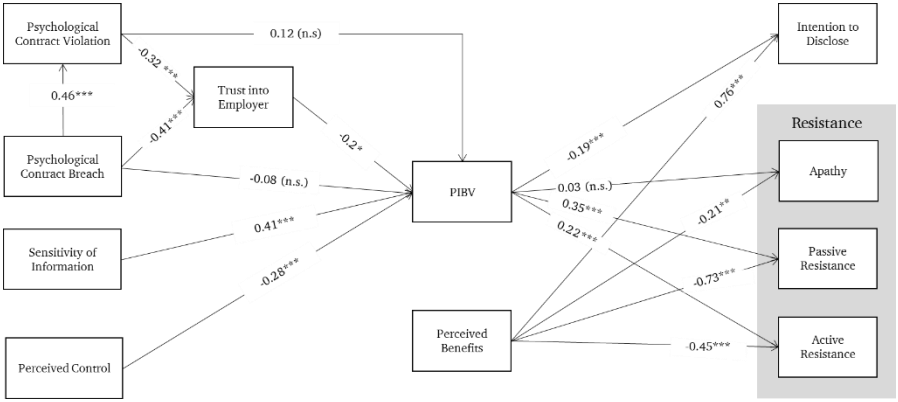


Figure 11: Results of Model Estimation

*** p ≤ 0.001; ** p ≤ 0.01; * p ≤ 0.05; (n.s.) p > 0.05

When testing for the significance of mediation, it is necessary to have a look on the confidence interval of the bootstrap analysis, as well as the p-value of the indirect path (see Subsection 5.6.1). The interval indicates a significance of the mediation when zero is not included in the interval. The p-value shows an evident mediation when the value is smaller than 0.05. As shown in Table 34 (based on Figure 12), the mean's indirect effect of the mediation of *Trust into Employer* on the relation between *Psychological Contract Breach* and *PIBV* is positive and significant (0.113; p-value < 0.05) with a 95% confidence interval excluding zero [0.02 - 0.21]. The direct effect c (-0.081) is not significant, as the p-value is greater than 0.05 and the confidence interval includes zero [-0.25 - 0.08]. In conclusion, the significance of the (a × b) effect and the insignificance of the (c) effect indicates that an indirect-only mediation is evident (H2-2 confirmed, H2-1 rejected). The same holds true for the mediating effect of *Trust into Employer* on *Psychological Contract Violation* and *PIBV*. The estimate of 0.136 with high significance (p-value < 0.05) and no zero in the confidence interval shows evidence of the hypothesis that trust is fully mediating the relationship (H1-2 confirmed, H1-1 rejected).

Effect	Estimate	Std. Error	P-Value	Confidence Interval
$(a \times b)$	0.113	0.06	0.023	[0.02 - 0.21]
(c)	-0.088	0.08	0.295	[-0.25 - 0.08]
$(d \times e)$	0.136	0.06	0.022	[0.02 - 0.26]
(f)	0.114	0.11	0.315	[-0.11 - 0.34]

Table 34: Bootstrap Analysis of Mediating Effect of *Trust into Employer*

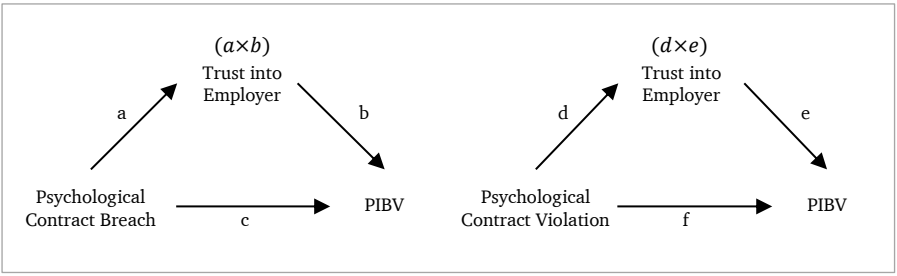


Figure 12: Mediating Effect of *Trust into Employer*

In the present model, the mediation is an indirect-only mediation as the direct relations (c) and (f) of Figure 12 are not significant due to p-value and confidence interval (see Table 34). The mediating effect fully explains the relationship between the independent variables *Psychological Contract Breach* and *Psychological Contract Violation* with *PIBV* and no direct relation could be found to be evident (see subsection 5.6.1).

5.8. Discussion of Intermediate Results

The goal of the study was to investigate the question if perceived information-based vulnerability of employees is influencing the usage behavior of employees of REIS, and how this perception is influenced by organizational and technological factors. For this purpose, the presented research model of subsection 5.4 and 5.5 was tested with survey data from the potential REIS user. The results of the data analysis show the fundamental interdependencies between technological influencing factors, organizational impact factors, fear for opportunism (PIBV), benefits and disclosure behavior of REIS user. In particular, it was found that PIBV has a major negative impact on the disclosure behavior of employees and a positive on the resistance behavior. Whereas the fear of opportunism is mitigated by benefit perceptions. Furthermore, technological factors have a decisive impact on the PIBV of employees. The organizational factor, trust, as well shows a significant impact on the employee's perception of opportunism on behalf of the employer, and furthermore, serves as a mediating effect for psychological contract breach and violation.

5.8.1. Contributions to Theory and Practice

Implications for Theory

The current study is one of the few scientific contributions on the sensitive information disclosure behavior of employees (see Section 3.1). Against this background, the present study provides a theory- and interview-based model that specifically identifies the value of technological and organizational aspects, such as trust and the psychological contract, as influencing factors on PIBV, and in turn the interplay of PIBV and benefit on disclosure and resistance behaviors of REIS users. This also takes account for the importance of interaction among perceived information-based vulnerability, as a privacy concern, and benefits on disclosure and resistance behaviors of employees. However, in the case of sensitive information disclosure research, such

a constellation has not been investigated in the employer context (see Section 3.1). In the course of sensitive information disclosure and related privacy research the main focus was on social network systems and e-commerce platforms as a software solution or application (e.g., Dinev and Hart 2006; Malhotra et al. 2004; White 2004). The results of the study provide evidence that a kind of calculus of benefits and concerns for privacy is not only of high relevance for the sensitive information disclosure behavior of employees but can influence their resistance behavior as well. This behavior has an even more serious impact on the success of REIS. For example, employees might tell co-workers to not use the system. In turn this could lead to a social norm to not use or even boycott the enterprise information system. PIBV was shown to prevent or reduce a disclosure and strengthen resistance. Thus, the study results demonstrate that, apart from disclosure intention, knowledge about resistance intentions might also be a useful insight for the success of REIS in particular but probably as well for e-commerce or social network systems.

It has been demanded by researchers that privacy research should be extended beyond consumer settings into organizational contexts and behaviors (Bélanger and Crossler 2011; Smith et al. 2011). The study shows that the perceived information-based vulnerability of employees, as a privacy concern, is a counterweight to benefits of a REIS solution. As Privacy Calculus Theory states that users' information sharing behavior depend on the benefits as well as the costs (e.g., risk beliefs or privacy concerns) associated with disclosure (Culnan and Bies 2003; Dinev and Hart 2006; Laufer and Wolfe 1977), this research contributes to the Privacy Calculus Research in the organizational context. It can be confirmed that the calculus of perceived benefits and perceived costs of disclosure also holds true for the organizational context, even though the costs are expressed in the perceived vulnerability through information disclosure.

With regard to the organizational context, the study also encompasses organizational factors that influence an employee's sensitive information disclosure behavior. The employer-employee relationship has an impact on the employee's fear of opportunism of the employer when deciding to disclose information or not. In particular, the effects of the existence of a psychological contract breach and violation on PIBV through trust in the employer were found to be significant. The study results suggest that employees may perceive vulnerability because of psychological breaches and violations, and a resulting weak trust relationship, which can ultimately be a major influencing factor on the disclosure behavior of employees in REIS.

Within the scope of the data analysis, all research hypotheses except H1-1, H2-1, and H6-2 could be confirmed. H1-1 and H2-1 were the direct positive effects of the psychological contract breach (H1-1) and violation (H2-1) on the perceived information based vulnerability. Nevertheless, the indirect mediating effects through trust was found to be significant. However, the study result is a contradiction to the qualitative research results of Section 4. Employees might have answered socially desirable, or in other words – they replied in a way that did not make them vulnerable because of sensitive information disclosure. Thus, employees might have perceived PIBV when they responded to the survey. Even though there is no proof for that theory, several observations

were found that support this notion. First, employees indicated psychological contract breaches in the previous qualitative research study and pointed out that their employer has broken and even violated the contract by behaving opportunistically (see Section 4). However, the average response behavior of psychological contract breach (average = 2.61) and violation (average = 1.56) was rather low, compared to other independent variables which did not focus on the employer-employee relationship (see Table 32). Hence, employees replied that they did not perceive any breach or violation of the psychological contract in the quantitative study, whereas the qualitative study indicates differently. Third, due to data security guidelines, the questionnaire of this study was done with a tool hosted by the company. It had the corporate design and a logo of the employer in the survey layout (see Figure 13), as well as in the invitation mail (see Figure 14, marked in Red). As the name of the employer and its corporate design, as well as its branding appeared quite often in the study, employees might perceive that the employer has access to the data, even though this was not the case and furthermore pointed out to the employee that data is treated secure and private.

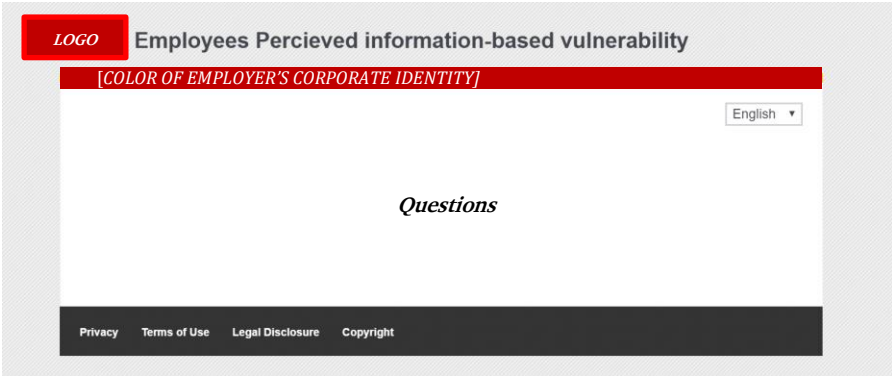


Figure 13: Survey Design and Layout

The last indication is the received e-mails from potential respondents, who pointed out that this survey was perceived as a threat or possible source for vulnerability when disclosing information.

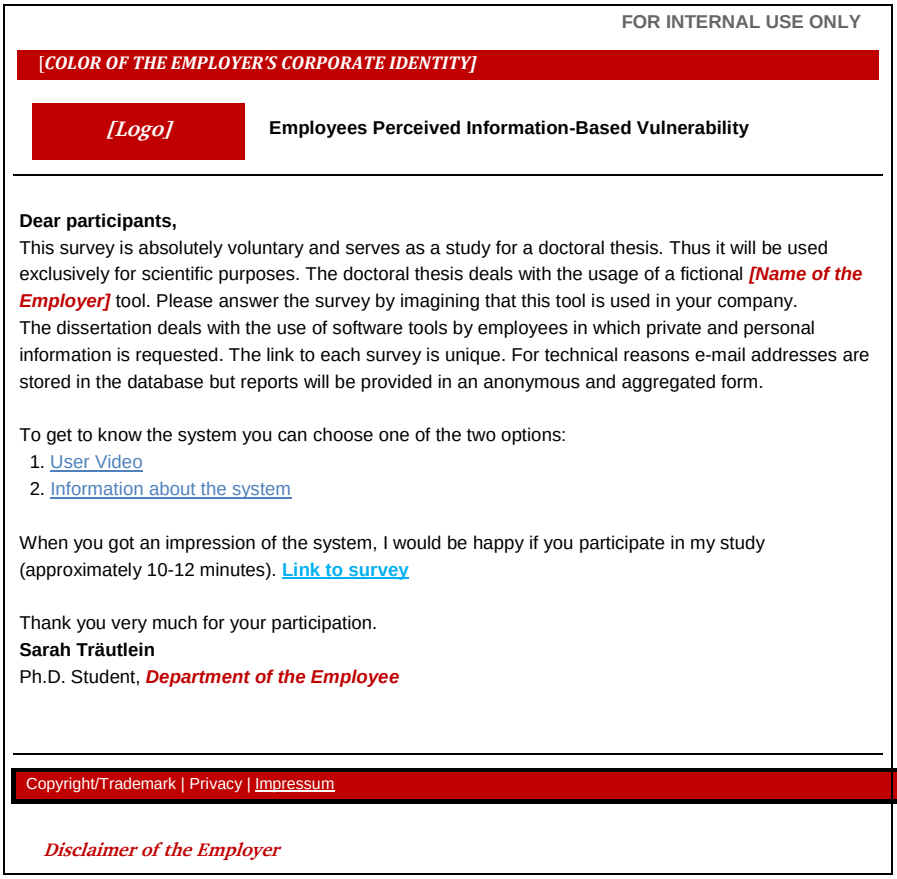
> *'[…] now I am looking through the questionnaire and see that the questions are not related to the software tool, but to my relationship with my employer. It really does not deal with the topic. I do not participate in the survey.' -Peter*

For instance, James even pointed out that there might be a preconceived notion in the results, as people who are generally suspicious might not answer the survey truthfully:

> *'The questions in the survey are quite personal in nature. It seems likely that colleagues who are critical of data protection issues in the evaluated tool will be cautious in the survey as well. Could be that there is a systematic distortion in the results. Personally, I had the impression that it [the survey] might be an investigation into how much data someone is willing to provide for a survey.' -James*

All these observations and hints for potential perceived vulnerability of employees through information disclosure showed the fear of people to answer truthfully on critical questions about the employer-employee

relationship. Thus, the rejection of hypotheses H1-1 and H2-1 should be rated with these facts in mind. However, this cannot be ascertained with confidence and should, therefore, be checked by further studies.


FOR INTERNAL USE ONLY

[COLOR OF THE EMPLOYER'S CORPORATE IDENTITY]

[Logo]

Employees Perceived Information-Based Vulnerability

Dear participants,
This survey is absolutely voluntary and serves as a study for a doctoral thesis. Thus it will be used exclusively for scientific purposes. The doctoral thesis deals with the usage of a fictional ***[Name of the Employer]*** tool. Please answer the survey by imagining that this tool is used in your company.
The dissertation deals with the use of software tools by employees in which private and personal information is requested. The link to each survey is unique. For technical reasons e-mail addresses are stored in the database but reports will be provided in an anonymous and aggregated form.

To get to know the system you can choose one of the two options:
1. User Video
2. Information about the system

When you got an impression of the system, I would be happy if you participate in my study (approximately 10-12 minutes). **Link to survey**

Thank you very much for your participation.
Sarah Träutlein
Ph.D. Student, ***Department of the Employee***

Copyright/Trademark | Privacy | Impressum

Disclaimer of the Employer

Figure 14: Invitation Mail

Furthermore, the hypotheses that PIBV has a positive impact on apathy (H6-2) could also not be confirmed. Nevertheless, it could be shown that resistance is additionally to intentions to disclose a major outcome from the calculus of PIBV and benefits of disclosure. Even though, the relationship between PIBV and apathy, as the lowest level of resistance, has no significance, the two remaining levels of resistance show high significance. The results illustrate that passive and active resistance are decisive outcomes of the privacy calculus of REIS. This means that it is important to consider resistance levels apart from disclosure behavior in organizational Privacy Calculus research.

The present model is particularly relevant for the implementation, development, and managing of EIS that have the main goal of revealing sensitive information from employees. Therefore, a new class of EIS was identified – namely, REIS. Characteristics of such systems, are that the employee actively discloses information into the system; the disclosed information tempts misuse and opportunism; and the success of the system depends on honest information provision of the employee. Thus, REIS subsumes EIS which require their users to make revealing information about themselves available to the organization for the system to be successful. In the daily work of an employee, several applications can be considered as REIS. For example, enterprise social networking platforms, wikis, (micro-)blogs, and other knowledge sharing systems or location-based mobile services can make employees perceive that they are revealing information (e.g., their activities or opinions). Besides, HR and workplace analytics tools, as well as employee mood measurement applications can also be counted to this class of EIS. Employees actively have to decide whether to disclose accurate and honest information into these systems or not.

Implications for Practice

As organizations increasingly adopt innovative technologies for interaction, collaboration, and HR analytics while possibilities for fast, creative, and automated data analysis grow, the success of systems such as REIS will be more and more dependent on the relationship quality between the employer and employee. Companies investing in the development and introduction of REIS need to consider their relationship with the employee to obtain value from these systems. This research presents a valuable contribution by pointing toward the peculiarities of REIS success and helps organizations to better deal with the implementation from the beginning.

REIS offer many benefits to employees and the organization, as they generate visibility and transparency regarding the employee's knowledge, activities, preferences, and social network connections (Treem and Leonardi 2013). Nevertheless, these benefits can only be generated if employees are willing to persist revealing information within REIS. This will only happen if employees perceive a benefit from disclosure, which outweighs their fear for opportunism. Even though organizations may not intend to be opportunistic at all, the question is whether employees subjectively misjudge their company's intentions in the context of their personal framing of REIS. All in all, REIS can offer many benefits for all stakeholders, when they are applied and perceived in the intended way. Nevertheless, several potential pitfalls might prevent stakeholders from using the system properly. As found in this study, potential difficulties coming along with REIS introduction and usage can be derived from the employer-employee relationship and characteristics of the system, such as perceived control and information sensitivity.

Moreover, companies should consider the fact that not only the refusal to use a REIS could be a consequence of PIBV, but also resistance against the system. Resistance could lead to a serious loss of money, as employees could resist by badmouthing the implementation and trying to prevent other people of the workforce to use the system as well. Thus, resistance has the potential to lead to a social norm of not using REIS. Companies should invest in countermeasures of this behavior and foster the workforce's intention to disclose, by investing in the

communication of benefits of a software solution and weakening PIBV by engaging in the improvement of the employer-employee relationship through trust measures in the long run.

Finally, the results of the study imply that that not only the characteristics of REIS are important to manage and to communicate to the employees, but companies should also invest in their relationship to the employee. This is especially important because a healthy psychological contract and building trust are not easy to achieve and require lengthy and costly investments by the employer into the workforce. Nevertheless, this investment is not only helpful for the implementation of REIS but for the whole company culture. Companies have to learn how the psychological contracts of employees look like and how they can fulfill, or at least know how to conduct, expectation management. Possibly, richer employer-employee communication can reduce PIBV through the exchange of information about the system and about the reciprocal obligations. It is crucial for success that both parties have realistic expectations of the system's implementation.

5.8.2. Limitations and Further Research

The present study should not be interpreted without considering its limitations. First, the data for the verification of the model stems from only one source. This was on the one hand necessary to investigate the psychological processes that are entirely within an individual and related to a company. On the other hand, the use of data from one source implies the possibility of distortion according to a Common Method Bias (MacKenzie et al. 2011; Podsakoff et al. 2012). Although the described measures in Sections 5.6.1 were designed to avoid such distortion, the use of different data sources or the temporal sharing of data collection would be a desirable addition to future research projects.

Furthermore, this study investigated the data from distinct conceptual perspectives, whereas other scientific perspectives have been neglected. With regard to the literature review of Section 3 and the findings of Section 4, the Privacy Calculus and Technological Frames perspective were a natural starting point to investigate this topic. However, taking further perspectives on sensitive information disclosure in REIS or EIS into account might help to furthermore understand the intentions of employees and shed light into their behavior.

Moreover, the usage of a non-related survey tool to the company would be desirable, as the formal layout and invitation might cause an impression that the employer could process the collected data. Thus it can be assumed that employees tended to answer critical questions about the employer-employee relationship strategically. This limitation goes in line with Podsakoff et al. (2003) that people tend to answer critical questions more positively and socially desirable. This tendency is perceived as problematic, as it can hide true relationships between constructs. For this research, this indicates that the not proven relationship between psychological contract breach or violation and PIBV could be caused by the employees' perception of vulnerability through disclosing in the survey, itself. For further studies, this implies that formal employer layouts should be avoided to prevent socially desirable answer patterns. Another possible

approach for avoiding PIBV can be the design of the items concerning the employer-employee relationship. Researchers could invest in a better fitting scale, which does not cause concerns of vulnerability from data provision itself, or collect the data by conducting an experimental study.

In order to carry out this study and to ensure a uniform understanding of REIS, the participants were presented with a concrete REIS solution. This is not necessarily representative of other REISs or the way in which they are perceived and used. It is necessary to check whether the results of this study are also valid with other REIS. Additionally, the present study was conducted on the basis of a fictional implementation of a REIS. Thus, no measures on behalf of the company took place to introduce the system. It can be expected that a real implementation process with strategic goals and communication would influence the employee's perception of the system and the related PIBV. Based on the provided user video and manual, employees were only able to find out about the content, handling, and purpose of the tested tool with the fact in mind that this solution will not be implemented in reality. For further studies, this implies that a real REIS implementation process should be accompanied by a PIBV study, to find out if the findings also hold true for real life cases.

An interesting question for future research would be if there are cultural differences among employees, perceiving REIS and using the systems. The present study focuses on employees employed in Germany. The consideration of international employees could help to generalize the findings of this research. Further studies could be conducted with regard to the location of a company or the culture where the organization is located. With regard to cultural differences, also personal differences, as values and preferences of employees could be integrated as influencers in the model. Identifying additional influencing factors could increase the understanding of how to prevent the occurrence of PIBV and related outcomes.

6. A Revealing Enterprise Information System Rollout – A Practical Implementation

6.1. Introduction

In the previous section, a theoretical model for the PIBV of employees and the resulting behavior was developed and evaluated. The results indicate that employees tend to disclose information when the perceived benefit from disclosure outweighs the perceived vulnerability trough disclosure. Otherwise, employees react with resistance against the system and do not contribute with information. Most likely their passive resistance against a REIS is influenced by the calculus of benefit and vulnerability. This means that employees would not use the system and would more or less ignore the fact that this specific REIS was implemented. Furthermore, results from the previous section also show that organizational factors, such as trust and partially the psychological contract, as well as system characteristics, have an impact on an employee's perception of PIBV. Hence, knowing these significant factors concerning the solution, as well as the relationship between the employee and the employer, that are influencing the REIS usage or resistance, can help companies to rollout these solutions properly.

To gain more insights on how a REIS implementation process can be supported by knowing the employees fear of opportunistic behavior and perceived benefit of enterprise solutions, this section describes a real introduction of a REIS and how this was supported by the findings of the PIBV survey. The REIS will be called *'People Involvement (PI)'* in this dissertation. The introduction took place in a Swiss sub-company of a globally acting company with headquarter in Europe, employing more than 10.000 employees. The primary goal of this section is to evaluate the PIBV potential of the system and its antecedents. Furthermore, it will be shown how and which measures should be derived to increase or foster the usage of REIS. It will be outlined, how the survey helps to introduce REIS in practice, by explaining the guidance on the implementation process and the related measures that were developed based on the study results. To evaluate the cause-effects of the employees' intention to disclose in PI, the applied questionnaire builds on the scientific model and evaluation of Section 5 but, however, is not scientifically correct, as the number of questions was reduced due to practical reasons. Furthermore, as indicators were found that the survey of the previous section had a PIBV potential, the design and application of the questionnaire was adapted accordingly. To reduce the potential PIBV of employees, the survey was conducted with the survey tool *Questback*, hosted by the University. Furthermore, the company's logo was excluded from the questionnaire and the invitation mail. As a further countermeasure, the logo of the university was included, which should highlight the scientific intentions of the study and, therefore, motivate employees to answer honestly without perceiving vulnerability through disclosure.

Hence, this section will deal with the question about the explanatory power of the influencing factors on the perceived information-based vulnerability, as well as PIBV on disclosure and resistance behavior of employees. Furthermore, related measures for implementation processes of REIS will be illustrated and discussed. Since PIBV is a system characteristic and therefore referring to the (planned) usage of a specific software solution, the data collection was directly

linked to the implementation of a representative software (PI). In the end, this section also gives more insights on the characteristics and peculiarities of REIS, as one typical solution, fulfilling these features, will be described in detail. For a better understanding of the project scope and the system characteristics, the following section gives a brief description of the frame of reference. Furthermore, the setting of the introduction and implementation of PI is going to be outlined. Afterwards, a description of the data analysis will be given. Therefore, the partial least square (PLS) methodology will be illustrated and contrasted to the covariance based approach of Section 5. The results of the analysis will be illustrated in Subsection 6.4. Furthermore, in Subsection 6.5 the derived and applied measures will be outlined. A Discussion of the findings is completing Section 6.

6.2. Frame of Reference of the Practical Study

This subsection gives an overview of the software solution in focus and the related project, which accompanied the rollout. PI is an in-house solution of the company and was developed in the headquarter in Europe. The Swiss sub-company was one of the first locations where this solution was implemented for first tests. The goal of the implementation was to gain insights on how the workforce accepted PI and furthermore to learn more about the usage behavior of employees. Therefore, the survey of this study served as an input source to find out more about the workforce's usage or resistance intentions.

6.2.1. Description of the REIS and the related Project – 'People Involvement'

People Involvement explains a new view on the human capital of companies. The focus is on employee satisfaction, motivation, engagement and their impact on the organizational success. This new conceptual approach is based on a 'value-oriented view' on employees. It supports the management to better judge on operational and strategic investment decisions in employees. Those investments in employees have to be targeted to the needs of employees, to increase employee engagement and to proof a related increased organizational success. The goal of PI is to generate value for the workforce, as well as the company. It enhances the communication between the workforce and the organization, by offering a basis to communicate about needs, obstacles, and disturbances at work and how to counteract them. The intention of PI is to engage people to improve business success and make employees feel happy at work.

Components of the solution 'People Involvement'

In order to fulfill these challenges, the PI solution consists of several components. The core of PI is a kind of questionnaire tool that reflects the needs of employees at the workplace. The employee has the possibility to create an individual needs profile. This profile consists of a selection of needs from a pre-defined needs-catalog, reflecting possible employee needs in the workplace. The employee selects workplace needs that are important for him. In the next step, the employee expresses how satisfied he is with these needs. Additionally, he can add a comment for further clarification. After saving the so called '*needs profile*', the data flows into aggregated reports and into the calculation of potential actions that increase the employee's satisfaction. The detailed profile remains only visible to the employee. Thus, other people of the company,

such as the employee's team, or the direct manager only have access to aggregated information on needs and their importance and satisfaction. The system ensures that no conclusions can be drawn about the needs of individual persons.

In the next step, the participating employee has the opportunity to take actions that help him to improve his satisfaction. The action proposal of the solution is based on the *'needs profile'* of the employee. These are suggested to the employee by means of a self-learning mechanism that is based on experiences. The mechanism learns by comparing similar *'needs profiles'* and the related conducted actions. An employee can also select own actions from an action catalog. For some measures, coordination with the manager is necessary (for example, due to budget approval). Therefore, the responsible manager also has access to the 'action suggestions' of the tool. A manager can get an overview of proposed actions for the team and individual employees. Furthermore, the suggestions of the tool help managers to discuss and conduct actions together with the employee.

Furthermore, reports are available at different levels of aggregation (e.g., reports for the employee about himself, his team and his organization, as well as anonymous company and manager reports regarding their teams or organizations). In compliance with applicable data protection guidelines, analyses can be carried out at different aggregation levels. By supplementing information on the organizational structure or demography of the workforce, further insights can be derived from the information for all stakeholders. Data can be illustrated in the course of time and compared with different aggregation levels. For instance, the satisfaction for teams can be compared with the whole organization in real-time. This can be used to identify current fields of action that can have a decisive influence on employee satisfaction. By constantly updating the data, all reports and key figures are calculated and displayed in real time.

'People Involvement' a Typical REIS

The solution PI is an exemplary solution for revealing enterprise information systems (REIS). When reconsidering the dominant characteristics of these solutions it gets obvious that PI can be classified as a REIS. First, the employee has to disclose sensitive information about his critical workplace needs and his related satisfaction into PI. Second, this provided information has high potential to serve mutual value, but as well tempts misuse and opportunistic usage of the employer. Third, the success of PI is dependent on the honest information provision by the employee, as usage refusal would lead to no possibilities to derive actions or get insights into statistics, to derive measures for better satisfaction management or corporate decisions at all. Hence, without information provisions companies, as well as employees cannot derive any value from the solution. However, if employees are willing to disclose information and not resist the usage, there is an enormous potential value and benefit for all stakeholders.

Along these opportunities for employees and companies, several obstacles are accompanying the solution. For instance, data protection regulations, employees' inherent mistrust in management, the fear of information misuse, or the concern of being ignored. To minimize the obstacles and

doubts, it is necessary to know how the employee perceives the information-based vulnerability of the system. Hence the nature regarding privacy of the technology, the benefits when using the system and the implementation intention of the employer play a decisive role in the acceptance and correct usage of the system.

6.2.2. Rollout of 'People Involvement'

To prevent expected pitfalls in advance, the rollout of PI was accompanied by a consulting team. The rollout phase started in September 2016 and lasted until December 2016. In this phase, 6 teams were introduced to the solution. An expert committee planned the step by step rollout of the solution. Rollout sessions with each participating team were arranged and conducted. Each session was led by two responsible experts of the committee. Every participant had the chance to ask questions and raise concerns in an open and transparent discussion. During the sessions, the solution, its goals, and the expected benefits for the employee were presented. After the introductory session, employees had the possibility to contact the committee through e-mail, telephone and directly in the system for asking further open questions. Furthermore, feedback loops were introduced. Responsible persons participated in team meetings to collect feedback on the employees' usage and impression of the system implementation.

The introduction of the solution was supported and promoted by the HR director of the company in Switzerland. However, the company's senior management was not actively involved in the rollout. After the complete rollout of the system, on average 0.5 employees inserted information into the system each day. This amount was equivalent to 53 contributions from employees during 110 days (12th of September 2016 to the 10th of February 2017; excluding weekends). As this ratio was lower than expected the committee decided to conduct a workshop, to find out why employees were not only rarely using the system. During this workshop, the results of the PIBV survey played a significant role in gathering insights on employees' perception about PI. The study revealed the employee's concerns and intentions to disclose or resist. On the basis of the results, discussions with the committee and several users were conducted, to derive useful measures.

6.3. Data Analysis

After two weeks of the introduction of PI, each employee received an e-mail invitation for the survey. As the tool was introduced in several rollout waves, one team after another, the data was collected between October 2016 and January 2017.

For the measurement validation and testing of the practical model, the Partial Least Square (PLS) method was applied. Generally, there are two ways to analyze structural equation models. The first is the covariance based approach, where constructs in a model are represented through factors (applied in Section 5); and the least square based approach, where components are representing constructs (PLS) (Lowry and Gaskin 2014). In comparison to the covariance analysis, the PLS method is more suitable for smaller data sets (Pavlou, Liang, and Xue 2007). Nevertheless, inadequate sample sizes can also result in problems in PLS (Lowry and Gaskin

2014). In the following, the PLS method will be described and the data collection process presented. In the end, the framework and the use case will be evaluated.

6.3.1. The Partial Least Square Method

As the covariance-based causal analysis (see Section 5.6.1), the partial least square approach serves the purpose of estimating causal relationships in structural equation models with latent variables (Gefen et al. 2000; Lowry and Gaskin 2014). The methodological difference of the PLS method is how the parameter estimation is performed. The regression analysis approach of least squares is conducted, where the model is decomposed into partial models (e. g., Lowry and Gaskin 2014). In contrast to the covariance-based causal analysis, in which the discrepancy between empirical and theoretical covariance matrix is minimized, the PLS method aims to maximize the stated variance of the dependent variables (e. g., Gefen et al. 2000; Lowry and Gaskin 2014). This results in a decisive decision-making factor – whether to conduct a variance (PLS) or covariance-based analysis. If the theory is at the center of the investigation a covariance-based method is useful. This means it should be judged how good theory can explain the empirical observations (e.g., Gefen et al. 2000; Lowry and Gaskin 2014). If on the other hand, the explanatory power of certain influencing factors is determined by one or more dependent variables, the PLS approach is a useful choice. In this case statements about the stated variance of the dependent variables can be made (Gefen et al. 2000).

Another difference between PLS and covariance-based causal analysis is the sample size required for the analysis. Since the PLS approach is based on the estimation of sub-models, a smaller number of parameters have to be estimated simultaneously. Hence, the method can also be applied with smaller sample sizes (e.g., Gefen et al. 2000; Haenlein and Kaplan 2004). Homburg and Klarmann (2006) recommend a sample size of at least 200 for the application of the covariance-based causal analysis. The PLS method requires that the number of observations should be at least ten times the number of independent variables that affect the dependent variable with the most influencing factors. Furthermore, the sample size should be at least ten times larger than the largest amount of indicators of a latent variable (Homburg and Klarmann 2006).

Since the parameter estimation of the PLS analysis is not performed simultaneously for the overall model, no global goodness-of-fit measures are available for assessing the model quality (e.g., Gefen et al. 2000). In return, the variance-maximizing method PLS allows the calculation of the coefficient of determination R^2. This is normalized at the interval [0,1] and is suitable for determining the explanatory power of the chosen influencing factors on a dependent variable (e.g., Gefen et al. 2000; Hair et al. 2006; Lowry and Gaskin 2014). For this purpose, each deviation of the observed dependent variable from the estimated value of the model parameters is examined. If a high proportion of the observed scattering can be explained by the model over the entire data set, the coefficient of determination has a high value. On the other hand, if the independent variables have little explanatory power on the dependent variable, the R^2 is smaller

(e.g., Hair et al. 2006). Formally, the coefficient of determination is calculated using the formula (Fahrmeir et al. 2016):

$$R^2 = \frac{Sum\ of\ Squares\ Explained}{Sum\ of\ Squares\ Total} = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y}_i)^2}$$

Whereas n is the amount of observations, y_i the observed value of the dependent variable of one observation, $\hat{y}_i$ the estimated model value of one observation i, and $\bar{y}_i$ the mean value of all observations. The coefficient of determination explains the proportion of the declared variance of a dependent variable explained by the model (Fahrmeir et al. 2016). In general R^2 values of approximately 0.67 are seen as substantial, values of approximately 0.33 as average, and values lower than 0.19 as weak (Urbach and Ahlemann 2010).

The PLS approach is a well-established method for evaluating structural equation models in IS research (e.g., Benlian and Hess 2011; Gefen et al. 2000; Lowry and Moody 2015; Posey et al. 2010; Venkatesh et al. 2003). Due to the limited sample size of the current practical study (n=56) and the question about the explanatory power of the organizational factors on the perceived information-based vulnerability, as well as PIBV on disclosure and resistance behavior, the PLS approach is applied.

6.3.2. Survey Design and Data Collection Process

A survey was designed to test the model, based on the questionnaire of Section 5. However, the survey of the previous section was reduced to a smaller set of questions. The reduction was perceived as necessary from the responsible committee, as the time investment for the survey should be reduced to a minimum. The reduction process was conducted during discussions with the HR director and the committee for the rollout. After several discussions, the survey was reduced from 45 to 31 questions, which seemed to be an acceptable amount of items for the committee (see Appendix E).

The short version was sent out with an e-mail distributor list of the solution. Hence, employees received the invitation from the solution itself and not from their employer. Furthermore, the survey was conducted with the tool Questback, which was hosted by the university and not by the company. The design was chosen based on the insights from the previous section, in order to prevent a possible PIBV (Figure 15).

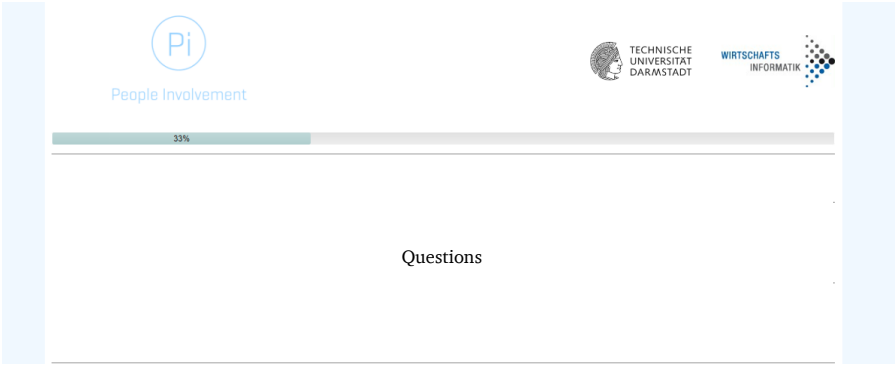


Figure 15: Design and Layout of the 'People Involvement' Survey

The recruitment of participants of the study happened in parallel to the rollout of PI. All potential users of the software were invited to fill out the survey after two weeks of the rollout meeting, to assure that employees had the opportunity to use the system already. Of the invited 226 participants, the response rate was 24.8% (56 participants). Whereas 33% were female, 66% male, and 4% remained unknown. Furthermore, the average age was 40 years, and the mean company affiliation was 8 years, whereas 1 was the lowest and 27 the highest amount of years, employees were with the company.

All participants received an invitation mail, which contained a short introductory section of the survey and a link to the questionnaire. The introductory section contained information about the approximate duration of the questionnaire (7 minutes), the information that all data will be processed anonymously and that it will not be possible to draw conclusions about the participants. To prevent PIBV, all information, enhancing the perception that the employer owned the survey or that the employer could have access to the data, was reduced to a minimum. Thus, the mail was sent from a distribution list of the software solution, the company sign was excluded, and it was highlighted that the data was gathered for a scientific study of a doctoral student.

6.4. Results of the Data Analysis

This section shows the outcomes of the data analysis of the survey results. First, the descriptive statistics will be illustrated and analyzed. Afterwards the PIBV model for 'People Involvement' will be presented.[9]

6.4.1. Descriptive Statistics and Correlation Analysis

Analogous to the procedure in Section 5.7.2, a descriptive investigation of the collected data was carried out by analyzing the mean value and standard deviation of each construct. Table 35 shows both statistics for the latent constructs of the current study.

[9] To protect the employees, due to regulations of the company the collected raw data will not be published.

Construct	Mean [a]	Standard Deviation
Sensitivity of Information	3.76	1.68
Perceived Control	3.77	1.70
Psychological Contract Breach	2.73	1.53
Psychological Contract Violation	1.90	1.37
Trust into Employer	5.21	1.54
PIBV	4.19	1.72
Perceived Benefits	4.59	1.43
Intention to Disclose	4.69	1.61
Apathy	3.19	1.70
Passive Resistance	2.85	1.73
Active Resistance	2.52	1.66

Table 35: Mean and Standard Deviation of Latent Variables

[a]: All variables were measured using a 7-point Likert-scale

Table 35 illustrates that all mean values are varying between 1.9 and 5.21. The standard deviations of the constructs vary between 1.37 and 1.72. A relatively low mean value of the psychological contract violation could be identified (1.9). This indicates that participants rated the violation of the psychological contract, caused by the employer, as rather low. Furthermore, employees rated their trust into the employer with a rather high average value of 5.21. The descriptive statistic indicates that employees tended to answer questions on their employer-employee relationship in a rather positive way with a high trust relationship and a low level of psychological contract breaches and violations. Furthermore, the PIBV and perceived benefits of employees reached a similar mean, whereas the average of the perceived benefits was slightly higher (PIBV=4.19; Benefits=4.59). Employees perceive potential vulnerability from disclosing in the system, but on average see a higher benefit than risk from the publication of information in PI. In addition, an employee's intention to disclose in PI was greater than their intention to resist the system. With an average intention of 4.69 employees would be willing to insert personal and private information in PI. As the average of resistance constructs was significantly lower, it can be expected that employees rather disclose information, than resist the system usage (see Table 35).

Constructs	1	2	3	4	5	6	7	8	9	10	11
1 Active Resistance	1.00										
2 Apathy	0.64***	1.00									
3 Intention to Disclose	-0.63 ***	-0.49 ***	1.00								
4 PIBV	0.54 ***	0.68 ***	-0.42 ***	1.00							
5 Passive Resistance	0.76 ***	0.71 ***	-0.70 ***	0.54 ***	1.00						
6 Perceived Benefits	-0.59 ***	-0.54 ***	0.57 ***	-0.46 ***	-0.62 ***	1.00					
7 Perceived Control	-0.43 **	-0.52 ***	0.43 ***	-0.62 ***	-0.57 ***	0.36 **	1.00				
8 Sensitivity of Information	0.37 **	0.37 **	-0.44 ***	0.40 **	0.39 **	-0.32 *	-0.51 ***	1.00			
9 Psych. Contract Breach	0.32 *	0.23	-0.44 ***	0.30 *	0.29 *	-0.47 ***	-0.37 **	0.35 **	1.00		
10 Psych. Contract Violation	0.35 **	0.33 **	-0.46 ***	0.36 **	0.33 *	-0.58 ***	-0.33 *	0.23	0.70 ***	1.00	
11 Trust into Employer	-0.48 ***	-0.55 ***	0.55 ***	-0.54 ***	-0.50 ***	0.52 ***	0.42 ***	-0.31 *	-0.63 ***	-0.71 ***	1.00

Table 36: Correlation Matrix of Latent Variables

*** $p \leq 0.001$; ** $p \leq 0.01$; * $p \leq 0.05$; n.s. $p > 0.05$

Table 36 shows the pairwise correlation coefficients between the latent constructs. Mostly all correlations are significant, except the correlation between *Psychological Contract Breach* and *Apathy*, as well as *Psychological Contract Violation* and *Sensitivity of Information*. A strong correlation is illustrated between the outcome variables *Passive Resistance* with *Active Resistance* (0.76), *Apathy* (0.71), and *Intention to Disclose* (0.70). Of particular interest are the relatively high and balanced correlations between *Benefits* with the outcomes, as well as *PIBV* and the examined outcomes. Both aspects correlate similarly with the behavioral intentions of the employees. This observation illustrates a relatively high significance of both aspects of the decision how to use PI.

6.4.2. Model Analysis

An investigation of the dependent variables offers information about the explanatory power of their respective influencing factors. The *PIBV* was explained by the *Perceived Control* and *Sensitivity of Information*, as well as the influencing factors stemming from the employer-employee relationship (*Trust into Employer, Psychological Contract Breach* and *Psychological Contract Violation*). The coefficient of determination R^2 assumes a value of 0.5. Thus, the influencing factors explain 50% of the variance of an employee's PIBV of the software PI in this simplified model. Both *PIBV*, as well as the *Perceived Benefits* of disclosure were modeled as influencing factors of the *Intention to Disclose* information in PI and could account for 36% of the variance of the dependent variable. Higher results were achieved for the explanatory power of *PIBV* and *Perceived Benefits* on *Passive Resistance* (47%) and *Active Resistance* (44%). Even though *PIBV* and *Perceived Benefits* explain nearly 53% of the variance of *Apathy,* the relation among these constructs was not significant.

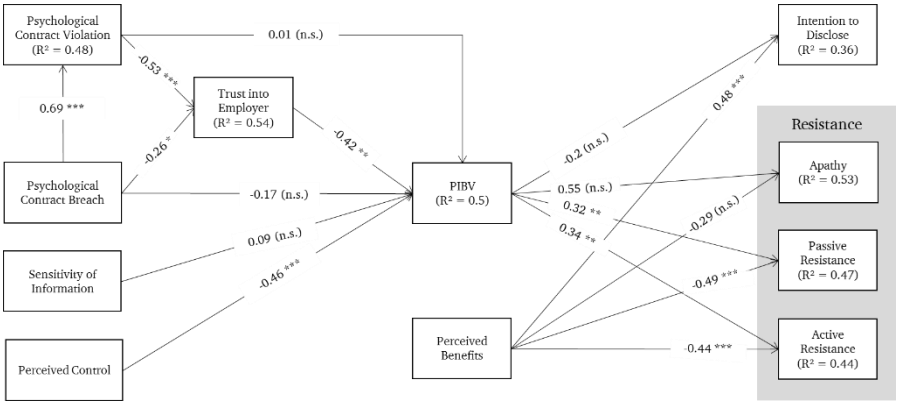


Figure 16: PLS Analysis of Simplified PIBV Model of 'People Involvement'

*** p ≤ 0.001; ** p ≤ 0.01; * p ≤ 0.05; n.s. p > 0.05

Figure 16 and Table 37 provide an overview of the results of the PLS analysis. Several significant relations could be identified for the usage of PI. For instance, the PLS analysis shows that

Perceived Benefits play a significant role when employees decide to insert information in PI. On the contrary, no significant relation could be identified for *PIBV* and *Intention to Disclose*. It can be concluded that when employees decide to disclose information in PI, they decide on the basis of the benefits, perceived when using the system. However, when taking a look at the resistance intentions of employees, it can be illustrated, that *PIBV* plays a decisive role in the decision whether to react with resistance against the system or not. This fact is highlighted by the highly significant relation between *PIBV* and *Passive Resistance* (0.32), as well as *PIBV* and *Active Resistance* (0.34). As well as *Intention to Disclose*, active and passive resistance are influenced by the perceived benefits of users. No significant relation could be identified between *PIBV* and *Apathy*, as well as *Perceived Benefits* and *Apathy*. Hence, when employees react with resistance against PI their perceived benefits and fear for opportunism have no impact on the apathy behavior. The PIBV of PI is on the one hand influenced by the perceived control of provided information into the system and on the other hand by the employer-employee relationship. *Trust into Employer* significantly influences the perceived vulnerability through information disclosure (-0.42).

Effect			Path coefficient	Significance Level	Result
Psych. Contract Violation	→	PIBV	0.01	0.943	Not Significant
Psych. Contract Violation (mediating effect of Trust into Employer)	→	PIBV	-0.53	0.000	Significant
Psych. Contract Breach	→	Psych. Contract Violation	0.69	0.000	Significant
Psych. Contract Breach	→	PIBV	-0.17	0.233	Not Significant
Psych. Contract Breach (mediating effect of Trust into Employer)	→	PIBV	-0.26	0.050	Significant
Trust into Employer	→	PIBV	-0.42	0.008	Significant
Sensitivity of Information	→	PIBV	0.09	0.422	Not Significant
Perceived Control	→	PIBV	-0.46	0.000	Significant
PIBV	→	Intention to Disclose	-0.2	0.120	Not Significant
PIBV	→	Apathy	0.55	0.207	Not Significant
PIBV	→	Passive Resistance	0.32	0.006	Significant
PIBV	→	Active Resistance	0.35	0.001	Significant
Benefits	→	Intention to Disclose	0.49	0.000	Significant
Benefits	→	Apathy	-0.29	0.181	Not Significant
Benefits	→	Passive Resistance	-0.49	0.000	Significant
Benefits	→	Active Resistance	-0.44	0.000	Significant

Table 37: Analyzed Effects of Simplified PIBV Model for 'People Involvement'

Furthermore, *Trust into Employer* fully mediates the effect between *Psychological Contract Violation* and *PIBV* (see Table 38). The mediating effect was tested in a bootstrap analysis, where the relation was found to be significant. With regard to the mediating effect of *Trust into Employer* on *Psychological Contract Breach* and *PIBV* no significant relation was found, as the confidence interval included zero (see Table 38).

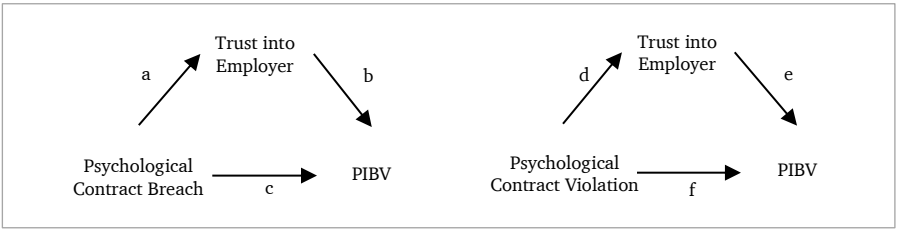


Figure 17: Mediating Effect of *Trust into Employer*

As already described in Section 5.6.1, when testing for the significance of mediation, it is necessary to have a look on the confidence interval of the bootstrap analysis, as well as the p-value of the paths. Mediation is significant when zero is not included in the confidence interval and the p-value is smaller than 0.05. As shown in Table 38 (based on Figure 17), the mean indirect effect of the mediation of *Trust into Employer* on the relation between *Psychological Contract Violation* and *PIBV* is positive and significant (0.22; p-value < 0.05) with a 95% confidence interval excluding zero [0.08 - 0.36]. The direct effect (f) (0.01) is not significant, as the p-value is greater than 0.05 and the confidence interval includes zero [-0.25 - 0.27]. In conclusion, the significance of the (d × e) effect and the insignificance of the (f) effect indicates that an indirect-only mediation is evident.

Effect	Estimate	Std. Error	P-Value	Confidence Interval
$(a \times b)$	0.11	0.1	0.27	[-0.08 - 0.3]
(c)	-0.17	0.16	0.2	[-0.47 - 0.14]
$(d \times e)$	0.22	0.07	0.002	[0.08 - 0.36]
(f)	0.01	0.13	0.94	[-0.25 - 0.27]

Table 38: Bootstrap Analysis of Mediating Effect of *Trust into Employer*

6.5. Derived Measures

Based on the results of the PLS analysis several measures were derived to increase the usage and disclosure intention of employees. During a one-day workshop, the results were discussed with stakeholders from the project. The HR management, as well as employees using the system participated in the workshop to conjointly analyze the low participation rate and afterwards derive important measures.

As the survey revealed that employees would not tend to resist the system but rather disclose information, when the benefit would be great enough, the team decided to concentrate on this fact. The committee did not perceive a fear that people might form coalitions against the system, as the mean answer rate of the resistance levels was rather low, compared to the intention to disclose (see Table 35). The goal was to derive measures about what could be done to increase the disclosure intention, by focusing on the question why employees did not perceive a benefit. During the workshop, the assumption that no perceived benefits were the actual cause of the low participation rate was confirmed. It got obvious that several aspects of the rollout phase resulted in the impression that benefits when using the system, were perceived as rather low. First, employees stated that they did not perceive senior management support of the solution 'People Involvement'. The people expected a commitment from the senior management and not only from the HR department, as they thought that a real value could only be generated when the head of the company in Switzerland would commit to the system and furthermore, take the feedback inserted into the solution serious. Even though the CEO of the company in Switzerland agreed with the rollout and supported the solution, no direct communication to the workforce was conducted from his side. Therefore, employees perceived the implementation as an *'HR frippery'*. Second, the same is valid for the commitment of the direct management. As the senior management did not communicate a commitment, the lower management also did not commit to the system. However, during the rollout two managers were convinced that the system could bring benefit to the team. This was reflected in their communication towards the teams in the team meetings. They regularly communicated their enthusiasm about the system to them and motivated them to ask questions about the solution to the present experts. As shown in Figure 18, those teams were the ones with the highest participation rate (see Figure 18, Team 4 & 5).

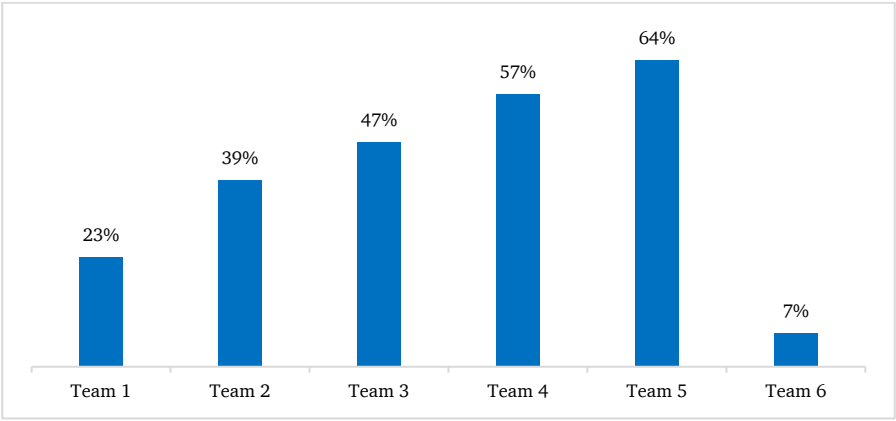


Figure 18: Usage-Log of 'People Involvement' on Team Level

Third, the timing of the rollout seemed to be unfortunate, as the official employee survey of the company was conducted at the same time period. The workforce perceived the well-known survey as the *solution of choice* of the senior management, and therefore ignored the

implementation of the solution 'People Involvement'. The workforce perceived that both solutions collected similar information and did not see the point in using both.

Based on these insights, the responsible rollout team could derive measures that should increase the participation rate:

1. A poster campaign was started to raise further awareness that the system could help employees to increase their work satisfaction easily.
2. To increase the commitment of the senior management, their communication team was involved in the discussions and the rollout committee.
3. The HR Executive planned to communicate derived insights from PI to the workforce. The communication should include the presentation of global measures based on the provided employee information. The goal was to show the benefit for the company and the entire workforce when using PI. Furthermore, they wanted to highlight that the employees' opinion and satisfaction was important for the organization.
4. As the buy-in of the lower management also seemed important, a further workshop with the direct management of the workforce was planned, to get their full support.
5. The HR management planned to link the results of the official employee survey with the satisfaction tool 'People Involvement'. The goal was to highlight that both solutions are essential for the company and that employees could have a benefit from using PI, even though they have already participated in the other survey.
6. Another measure was to better communicate the goal of the implementation of PI, in order to assure full transparency and to highlight that no hidden agenda was present.
7. As the responsible committee assumed that employees might feel uncertain and insecure with the new approach of gathering employee information in a transparent, real-time and open way, experts were sent out to the teams to present first results derived from the data in the solution for each group. The goal was to make people comfortable with the approach of collecting insights from information and learning from these findings.

6.6. Discussion of Intermediate Results

The analysis of the practical PIBV model of PI shows similar results as the previous study in Section 5. However, it should be considered that the data collection was conducted with a limited amount of questions, and the approach was not completely scientific. Furthermore, the amount of collected data points (n=56) is sufficiently high for PLS analysis, however, it is not significantly higher than the necessary amount of 50. The study served as an example of how the PIBV survey could be applied in practice and which helpful insights could be derived during the rollout of a REIS. Therefore, several implications for practice can be derived from the findings of this section. Furthermore, it helps to better understand the peculiarities of REIS, its implementation, and the related PIBV of employees regarding those systems.

6.6.1. Contributions to Practice

The derived measures of this section show that knowing the employee's drivers and inhibitors of using an enterprise information system helps to successfully implement those solutions.

Companies have to deal with the fact that REIS are enterprise information systems that need a planned and employee targeted rollout. Employees want to be involved in the implementation phase and want to have the feeling that the goals of the company, to implement REIS, are transparent. Moreover, employees need the feeling that their employer takes the implementation serious and that even the senior management is convinced of the mutual benefit of such systems. All stakeholders have to support and promote the solution. Otherwise, employees perceive missing additional value and potential fear from disclosure.

Companies should engage in transparent communication to prevent technological framing of the employee. If employees do not understand the implementation purpose, they start to interpret the purpose, which might lead to a negative frame. Therefore, transparent and comprehensible goal communication from the senior management to the workforce is recommended. The senior management is a key stakeholder. If REIS is only implemented and rolled out by the responsible line-of-business department (e.g., HR department), employees might perceive the solutions as a *'personal toy'* of that specific department and do not see the overall business value. This transparent communication should be personal and verbal. However, this direct communication should be supported by blogging, e-mails, or poster campaigns. Raising awareness about the REIS solution and the holistic support of the management is evident for employee's willingness to access and use the system. Furthermore, the direct management also plays a key role in the implementation process of REIS. For employees, the direct management often represents the company and its perspective. Therefore, if direct managers are not convinced of the benefit of such a solution, employees might not understand the value of such solutions at all. It was shown that the disclosure behavior of teams, where the direct manager supported the solution, was way higher than from other teams. Involvement and support of the direct management is evident for REIS success. Moreover, companies should communicate results of the usage of REIS. For instance, if an HR-Feedback system is introduced, the management should communicate results and insights as soon as possible. This helps to show the benefit of the solution and furthermore, strengthens the belief that the company communicates open and transparent. When employees contribute with sensitive information, they expect a benefit from it. Be it a personal or more global benefit. Companies should convince employees that their sensitive information disclosure contributes to a global purpose of the company and that employees can contribute to a positive change.

Furthermore, if similar solutions are already implemented in an organization, companies should either show the link between the different solutions or should communicate that the introduced REIS is the system that makes the difference. This study illustrated the challenges coming along with the application of two similar solutions at the same time. Employees were confused how these two approaches fit and link together. They did not see a meaning in using both solutions. Therefore, employees decided to use the well-known, old solution. As a countermeasure, results of both solutions should be integrated into one report and presented to the workforce.

Even though the derived measures of this section focused on the improvement of the disclosure intention of employees, the study also shows that it is important to take action regarding possible resistance against the system. As already found out in the previous section, passive and active resistance can lead to serious problems for REIS implementation. Employees could badmouth against the solution and therefore might establish a social norm of not using the system. Companies have to consider the fact that PIBV is a significant influencing factor that should be managed properly. Managing PIBV, however, is a long-term task. It relates to the employer-employee relationship, as well as technological characteristics of the solution. Especially managing the employer-employee relationship involves for example measures regarding organizational culture, trust relationship, and expectation management. Building a trustworthy culture, where everyone can speak up and is not feared of opportunism, is a costly and lengthy process (Galford and Drapeau 2003). However, on the long-term, these measures do not only support the rollout and implementation of REIS but as well might contribute to business success in general.

As shown in this study, several countermeasures can be derived from the model, to prevent non-usage of REIS. Companies should focus on a proper planned introduction of REIS solutions. If there are any concerns regarding the trust relationship between the workforce and the employer, early countermeasures should be conducted. A transparent and personal communication is a good starting point.

6.6.2. Limitations and Further Research

The present practical study has several limitations that should be considered. First, the data collection was conducted with a survey, which was not scientifically evaluated. Even though the underlying PIBV model is based on the evaluated and operationalized model of the previous section, the survey for data collection of this section was narrowed down due to practical aspects. Therefore, no implications for theory were given in this section. However, the model and the derived measures help to gain insights on the applicability of the questionnaire in practice and how it can support REIS implementation.

Second, this study was conducted in only one company. This was necessary, as the rollout process of the REIS was conducted in this specific company. However, one data source always implies the possibility of distortion according to a Common Method Bias (MacKenzie et al. 2011; Podsakoff et al. 2012). Although several measures were applied to prevent a bias (described in Section 5.6.1 and Section 6.3.2), the use of different sources or a temporal distribution of the data collection would additionally help to prevent biases. Furthermore, with regard to biased answering, it would help to decouple the survey completely from the company, as the factors related to the employer-employee relationship still represent critical questions for employees. Even though the insights and findings from the previous section were taken seriously and the design of the survey and introduction mail was changed, to prevent the impression that the company would have access to the data, employees still knew that 'People Involvement' was built in-house and therefore, also the survey was conducted by people within the company. For a

subsequent study, an independent company should be tested, where the REIS, as well as the PIBV survey, are not build or conducted in-house. This could furthermore help to prevent biased answering for sensitive questions.

Fourth, the amount of collected data (n=56) is on the bottom line of acceptable data points for a PLS analysis (see Section 6.3.1). The PLS method requires that the number of observations should be at least ten times the number of independent variables that affect the dependent variable with the most influencing factors. In this study, PIBV is the construct with the most items (five items) and has five influencing factors (see Figure 16). Therefore, the minimum amount of observations, with regard to this criterion, would be n=50. Another criterion is that the sample size should be at least ten times larger than the largest amount of indicators of a latent variable (Homburg and Klarmann 2006). With regard to the present model, also PIBV represents the construct with the most items (five items). With regard to this recommendation, the minimum amount of data points also should not be less than 50. Collecting more information would potentially help to increase the validity of this study for theory.

Fifth, the data collection was conducted after two weeks of each rollout phase. After approximately two months of the first rollout phase, the actual usage state was analyzed, and appropriate measures were derived. For an even more reliable and valid outcome of this practical study, a second evaluation of the usage and disclosure intention of employees would be helpful. It would help to show if the derived measures did really contribute to the employee's usage intention of the REIS.

7. Conclusion and Implications

In this dissertation the employee's willingness to disclose sensitive information in enterprise information systems was investigated. The present work shows that the introduction of revealing enterprise information systems not only leads to an increase in the employee's work performance and a more comprehensive consideration of their work behavior but can also have a contrary effect. For instance, employee's often feel that the provided information could be misused by their employer. Based on this knowledge, this dissertation discussed the *Perceived Information-Based Vulnerability (PIBV)* of employees in particular. Furthermore, the dissertation examined the resulting willingness to disclose sensitive information or develop strategies for resistance against those systems. This work contributes to the enhanced understanding of the implementation success of enterprise information systems and has several implications for theory and practice. Since these implications have already been discussed in detail in each section, a summary of the key results will be provided below.

7.1. Contributions to Theory

First of all, in this dissertation, a new construct, called *Perceived Information-Based Vulnerability (PIBV)*, was presented. It expresses the employee's fear that an employer might misuse the employee's disclosed information to the employee's disadvantage (Section 5). It could be shown that employees weigh between their PIBV and the perceived benefits of revealing information when deciding to disclose sensitive information or resist using the system. This calculus approach is derived from the Privacy Calculus Research (Dinev and Hart 2006) that is one of the fundamental theories of sensitive information disclosure in information systems. The present study extends Privacy Calculus Research into the direction of the organizational context.

To prevent non-usage or even destructive usage of EIS, employers need to incentivize high-quality usage and disclosure. This represents a crucial element for the success of REIS. It was found, that *Perceived Benefit* is the primary influencing factor on the intention to disclose sensitive information in the organizational context. This indicates that, even though, employees perceive potential vulnerability through information disclosure, they might reveal information when the expected benefit or outcome seems valuable. Perceived benefits outrange PIBV of REIS (Section 5 and 6).

Furthermore, in the present dissertation, factors were determined – based on theory and qualitative research – where a significant impact on the PIBV of employees and, therefore, their willingness to use enterprise information systems, was proven. Next to system characteristics, such as perceived control of the information or the sensitivity of requested information, factors expressing the employer-employee relationship were determined. In this research, a good employer-employee relationship is mirrored in the quality of the psychological contract of an employee and his trust relationship with the employer. If a psychological contract is perceived as broken or even violated, the trust relationship with the employer suffers. This lack of trust has a direct impact on the employee's PIBV.

In addition, this dissertation addressed alternative outcomes of the PIBV/benefit calculus. Apart from the employee's intention to disclose information, the possible serious outcome of resistance against EIS usage was introduced and evaluated. The results show that high PIBV and low perceived benefits can lead to either active or passive resistance. In the worst case, this is expressed through badmouthing against the software solution or even destructive behavior, which could lead to refusal of usage of the entire workforce (see Section 5 and 6).

Furthermore, this scientific work introduced a new class of enterprise information systems, called REIS. *Revealing Enterprise Information Systems* (REIS) emerge in the organizational world and also have to be considered in theory, as they exceed the traditional research of technology acceptance (see Section 5). Several peculiarities of REIS and the related sensitive information disclosure behavior of employees could be identified during this dissertation. In particular, these enterprise software solutions have a high possibility for PIBV and, therefore, were well suited as exemplary solutions for this research.

With regard to the literature review, this dissertation offers an exhaustive overview and examination of scientifically relevant literature on *Sensitive Information Disclosure* (SID) (Section 3). During the review, it could be shown that research on SID mainly focuses on social network systems and e-commerce websites, where disclosure of sensitive information is highly relevant for business success. Furthermore, it was found that the construct is mainly applied in Privacy Calculus Research, where SID was a dominant dependent variable of the calculus of privacy risks or concerns and perceived benefits. In addition to that, the review provides an exhaustive overview and examination of possible influencing factors on SID, based on the scientific literature.

7.2. Contributions to Practice

In addition to the scientific implications described above, conclusions from the present dissertation can also be derived for corporate practice.

First, the present work illustrated that the perceived information-based vulnerability and the perceived benefits of a revealing enterprise information system influence the intention to disclose sensitive information or react with resistance against those systems. Since people weigh between benefits and costs when deciding to step into a relationship (Metzger 2004), employees weigh between perceived benefits of self-disclosure and their fear of information misuse when disclosing information (PIBV). In fostering the awareness about the potential benefits for employees, companies can achieve a higher contribution rate. As illustrated in the practical study, organizations can engage in campaigns and success stories.

However, the practical case in Section 6 has also illustrated that an introduction of a REIS should be supported by all stakeholders of a company. Especially the senior and direct management has to be convinced that such a solution has a value add for the company and the workforce. Otherwise, employees might have problems to understand the benefit of such solutions.

Transparency and open communication about benefits and potential concerns of the workforce are good countermeasures that help these solutions to become more successful.

Third, the fear of opportunistic behavior and vulnerability through self-disclosure was shown to be influenced by the characteristics of a REIS and the employer-employee relationship. In this thesis, it has been revealed that individuals who have a good employer-employee relationship, expressed in trust in the employer and a healthy psychological contract, react with a lower perception of vulnerability through information disclosure. These feelings increase the intention to disclose and ultimately decrease the potential for resistance against the system. Possible implications for the implementation process can be derived from these findings. Since trust-driven relationships are easier to manage than exchanges that are driven by concerns and fears (Pavlou and Gefen 2005), companies should engage in the prevention of psychological contract violations and take countermeasures to avoid misunderstandings from materializing into violations of the contract. Furthermore, companies should focus on expectation management regarding the content of the psychological contracts of employees, to prevent frustration and disappointment in advance, which might lead to mistrust and higher PIBV.

Additionally, the perceived information-based vulnerability of employees is ultimately influenced by the sensitivity of requested information and the perceived control over the information in the system. These two aspects represent system characteristics, which are sometimes hard to change, as they are already specified in the software solution. However, companies should engage in the evaluation of the workforce's readiness to contribute specific information types in advance, before they implement REIS. Many REIS might need advised and precisely planned rollouts. The practical study of Section 6 illustrated that individuals have to be introduced to the system in small groups where everyone can raise his concerns and speak up. Following this way, companies can achieve the highest impact, as employees better understand the intention behind the implementation and what companies want to do with the disclosed sensitive information. Knowing about employees' concerns enables organizations to address them directly.

Moreover, this dissertation examined the extent to which employees might react with apathy, passive resistance, or active resistance on the implementation of REIS and how it is affected by the calculus of benefits and PIBV. In particular, a central role of passive and active resistance could be observed. Thus, companies should consider these reactions, as in particular, active resistance can result in opposing behavior by blocking and impeding REIS implementations (Coetsee 1999). This can be expressed in voicing out strong opposing views and attitudes to other people of the workforce. Countermeasures, by strengthening the awareness about benefits and fostering the relationship to the employee can help to prevent such reactions.

In the end, it should be noted that not the real intention of REIS implementation by the company is crucial for the success, but rather the purpose that employees perceive behind the implementation. Experiences from the past, the company's communicated implementation

strategy, perceived benefits and the nature of the technology shape this subjective opinion. This is an important insight for enterprises. Companies have to understand the workforce's perspective and their point of view on the system. When implementing REIS they should be transparent about their implementation goals and communicate them in a clear and compelling way. This can prevent the employee's own interpretation about a possible hidden agenda of the employer. When employees start interpreting, negative frames about solutions might arise and lead to non-disclosure or even resistance.

7.3. Future Research

With respect to the research on sensitive information disclosure of employees in enterprise information systems, there are still several open questions which should be tackled in future studies. In closing this work, essential further challenges for the implementation success of revealing EIS and thus approaches for future studies will be portrayed.

First, the dissertation is a first step in the direction for better understanding information disclosure behavior of employees in EIS. Nevertheless, further research should be conducted in this regard, as the final model was limited to the Privacy Calculus Theory, enriched with Psychological Contract and Technological Frames Theory. Further aspects of other theories could be considered in the future. These aspects can help to gather more insights on the topic. Second, with regard to Privacy Calculus Research, the present studies have illustrated that there are further outcomes, concerning the calculus, then information disclosure intentions. It was found that resistance plays a significant role. Further research should be conducted to gather more insights on the resistance behavior of employees as outcome of a cost/benefit calculus. Third, the construct trust into the employer should be investigated in more detail. The study of Section 4 illustrates that trust toward upper levels of management seemed to affect the employee's attitudes toward ESS greatly, whereas the trust relationship of employee and direct management appeared to have a lower impact. This presents an interesting perspective as REIS are often aimed at fostering information sharing across hierarchy levels and thus should break up strict company structures. As outlined above, this goal might be difficult to achieve if trust relationships are absent across hierarchy levels. Thus, further research could focus on investigating in the trust construct by distinguishing trust into senior and direct management levels in the employee's sensitive information disclosure intention context.

In the end, the following limitations should be considered: first, the data collection of this dissertation was from a single large multi-national company. Further similar studies are needed in additional enterprises to find out whether the results are biased by the single company approach. Second, only one REIS was tested. Therefore, further studies should also be conducted in this regard. The structural equation model should be applied for additional enterprise information systems, or even REIS. Third, the data collection was only conducted in German and Swiss subsidiaries. For further generalization of the findings, data should be collected in additional countries.

Bibliography

Ajzen, Icek. 1991. “The Theory of Planned Behavior.” *Organizational Behavior and Human Decision Processes* 50(2):179–211.

Alimam, Mayla, Emmanuel Bertin, and Noel Crepi. 2015. “Enterprise Social Systems: The What, the Why, and the How.” in *Proceedings of the 17th Conference on Business Informatics*.

Allen, Watkins M., Stephanie J. Coopman, Joy L. Hart, and Kasey L. Walker. 2007. “Workplace Surveillance and Managing Privacy Boundaries.” *Management Communication Quarterly* 21(2):172–200.

Altman, Irwin and Dalmas A. Taylor. 1973. *Social Penetration: The Development of Interpersonal Relationships.* Oxford, England: Holt, Rinehart & Winston.

Anderson, Catherine L. and Ritu Agarwal. 2011. “The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information.” *Information Systems Research* 22(3):469–490.

Andrade, Eduardo B., Velitchka Kaltcheva, and Barton Weitz. 2002. “Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation.” *Advances in Consumer Research* 29(1):350–353.

Angst, Corey M. and Ritu Agarwal. 2009. “Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion.” *MIS Quarterly* 33(2):339–370.

Babbie, Earl. 2010. *The Practice of Social Research*. 12th ed. Belmont, CA: Wadsworth.

Bagozzi, Richard P. and Lynn W. Phillips. 1982. “Representing and Testing Organizational Theories: A Holistic Construal.” *Administrative Science Quarterly* 27(3):459–489.

Bansal, Gaurav, Fatemeh M. Zahedi, and David Gefen. 2010. “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online.” *Decision Support Systems* 49(2):138–150.

Barki, Henri, Ryad Titah, and Celine Boffo. 2007. “Information System Use-Related Activity: An Expanded Behavioral Conceptualization of Individual-Level Information System Use.” *Information Systems Research* 18(2):173–192.

Baron, Reuben M. and David A. Kenny. 1986. “The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual , Strategic , and Statistical Considerations.” *Journal of Personality and Social Psychology* 51(6):1173–1182.

Bélanger, France and Robert E. Crossler. 2011. “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.” *MIS Quarterly* 35(4):1017–1041.

Bélanger, France, Janine S. Hiller, and Wanda J. Smith. 2002. “Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes.” *Journal of Strategic Information Systems* 11(3):245–270.

Benlian, Alexander and Thomas Hess. 2011. “Opportunities and Risks of Software-as-a-Service: Findings from a Survey of IT Executives.” *Decision Support Systems* 52(1):232–246.

Berger, Peter L. and Thomas Luckmann. 1967. *The Social Construction of Reality*. New York, New York: Doubleday.

Berghaus, Sabine and Andrea Back. 2014. “Adoption of Mobile Business Solutions and Its Impact on Organizational Stakeholders.” in *Proceedings of the 27th BLED eConference*.

Birnholtz, Jeremy, Graham Dixon, and Jeffrey Hancock. 2012. “Distance, Ambiguity and Appropriation: Structures Affording Impression Management in a Collocated Organization.” *Computers in Human Behavior* 28(3):1028–1035.

Bowie, Norman E. and Karim Jamal. 2015. “Privacy Rights on the Internet: Self-Regulation or Government Regulation?” *Cambridge University Press* 16(3):323–342.

Bregman, Alvan and Caroline Haythornthwaite. 2003. “Radicals of Presentation: Visibility, Relation, and Co-Presence in Persistent Conversation.” *New Media & Society* 5(1):117–140.

vom Brocke, Jan et al. 2009. “Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process.” in *Proceedings of the 17th European Conference on Information Systems*.

Brown, Steven D. and Geoffrey Lightfoot. 2002. “Presence, Absence, and Accountability: Email and the Mediation of Organizational Memory.” in *Virtual Society? Technology, Cyberbole, Reality*, edited by S. Woolgar. Oxford, England: Oxford University Press.

Brown, Timothy A. 2015. *Confirmatory Factor Analysis for Applied Research*. 2nd ed. New York, New York: The Guilford Press.

Buettner, Ricardo. 2015. “Analyzing the Problem of Employee Internal Social Network Site Avoidance: Are Users Resistant due to Their Privacy Concerns?” in *Proceedings of the 48th Annual Hawaii International Conference on System Sciences*.

Bughin, Jacques. 2015. “Taking the Measure of the Networked Enterprise.” *McKinsey Quarterly*. Retrieved February 5, 2017 (http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/taking-the-measure-of-the-networked-enterprise).

Bughin, Jacques, Michael Chui, and Andy Miller. 2009. *How Companies Are Benefiting from Web 2.0: McKinsey Global Survey Results*.

Buhse, Willms and Sören Stamer. 2008. *Enterprise 2.0 - The Art of Letting Go*. Bloomington, New York: iUniverse.

Buregio, Vanilson, Zakaria Maamar, and Silvio Meira. 2015. “An Architecture and Guiding Framework for the Social Enterprise.” *IEEE Internet Computing* 19(1):64–68.

Burton-Jones, Andrew and Camille Grange. 2012. “From Use to Effective Use: A Representation Theory Perspective.” *Information Systems Research* 24(3):632–658.

Burton-Jones, Andrew and Detmar W. Straub Jr. 2006. “Reconceptualizing System Usage: An Approach and Empirical Test.” *Information Systems Research* 17(3):228–246.

Caya, Patty and Jakob Nielsen. 2009. *Enterprise 2.0: Social Software on Intranets*. Nielsen Norman Group.

Charki, Mohamed Hédi and Emmanuel Josserand. 2008. “Online Reverse Auctions and the Dynamics of Trust.” *Journal of Management Information Systems* 24(4):175–197.

Chatterjee, Samprit and Ali S. Hadi. 2015. *Regression Analysis by Example*. Hoboken, New Jersey: John Wiley & Sons.

Chen, Rui and Sushil K. Sharma. 2013. “Self-Disclosure at Social Networking Sites: An Exploration Through Relational Capitals.” *Information Systems Frontiers* 15(2):269–278.

Chui, Michael et al. 2012. “The Social Economy: Unlocking Value and Productivity through Social Technologies.” *McKinsey Global Institute*.

Churchill, Gilbert A. 1979. “A Paradigm for Developing Better Measures of Marketing Constructs.” *Journal of Marketing Research* 16(1):64–73.

Churchill, Gilbert A. and Dawn Iacobucci. 2005. *Market Research: Methodological Foundations*. 9th ed. Mason, Ohio: Thomson South-Western.

Coetsee, Leon. 1999. “From Resistance to Commitment.” *Public Administration Quarterly* 23(2):204–222.

Collins, Nancy and Lynn Miller. 1994. “Self-Disclosure and Liking: A Meta-Analytic Review.” *Psychological Bulletin* 116(3):457–475.

Coltman, Tim, Timothy M. Devinney, David F. Midgley, and Sunil Venaik. 2008. “Formative versus Reflective Measurement Models: Two Applications of Formative Measurement.” *Journal of Business Research* 61(12):1250–1262.

Conway, Neil and Rob B. Briner. 2005. *Understanding Psychological Contracts at Work: A Critical Evaluation of Theory and Research*. Oxford, England: Oxford University Press.

Culnan, Mary J. and Pamela K. Armstrong. 1999. “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10(1):104–115.

Culnan, Mary J. and Robert J. Bies. 2003. “Consumer Privacy: Balancing Economic and Justice Considerations.” *Journal of Social Issues* 59(2):323–342.

Davidson, Elizabeth. 2006. “A Technological Frames Perspective on Information Technology and Organizational Change.” *The Journal of Applied Behavioral Science* 42(1):23–39.

Davidson, Elizabeth and David Pai. 2004. “Making Sense of Technological Frames: Promise, Progress, and Potential.” Pp. 473–91 in *Information Systems Research: Relevant Theory and Informed Practice*, edited by B. Kaplan, D. P. Truex, D. Wastell, A. T. Wood-Harper, and J. I. DeGross. Springer US.

Davis, Fred D. 1989. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.” *MIS Quarterly* 13(3):319–340.

Deery, Stephen J., Roderick D. Iverson, and Janet T. Walsh. 2006. “Toward a Better Understanding of Psychological Contract Breach: A Study of Customer Service Employees.” *Journal of Applied Psychology* 91(1):166–175.

DeLone, William H. and Ephraim R. McLean. 2003. “The DeLone and McLean Model of Information Systems Success: A Ten-Year Update.” *Journal of Management Information Systems* 19(4):9–30.

Denyer, David, Emma Parry, and Paul Flowers. 2011. “ ‘Social’, ‘Open’ and ‘Participative’? Exploring Personal Experiences and Organisational Effects of Enterprise 2.0 Use.” *Long Range Planning* 44(5):375–396.

Derlega, Valerian, Sandra Metts, Sandra Petronio, and Stephen T. Margulis. 1993. *Self-Disclosure*. Thousand Oaks, California: Sage Publications.

DeVellis, Robert F. 2016. Scale Development: Theory and Applications. 26th ed. edited by L. Bickman and D. J. Rog. Sage Publications.

Diamantopoulos, Adamantios and Heidi M. Winklhofer. 2001. “Index Construction with

Formative Indicators: An Alternative to Scale Development." *Journal of Marketing Research* 38(2):269–277.

DiMicco, Joan et al. 2008. "Motivations for Social Networking at Work." in *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*.

Dinev, Tamara, Jahyun Goo, Qing Hu, and Kichan Nam. 2009. "User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences." *Information Systems Journal* 19(4):391–412.

Dinev, Tamara and Paul Hart. 2004. "Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model." *Behaviour & Information Technology* 23(6):413–22.

Dinev, Tamara and Paul Hart. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17(1):61–80.

Dinev, Tamara, Paul Hart, and Michael R. Mullen. 2008. "Internet Privacy Concerns and Beliefs about Government Surveillance - An Empirical Investigation." *Journal of Strategic Information Systems* 17(3):214–233.

Dinev, Tamara, Heng Xu, H.Jeff Smith, and Paul Hart. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." *European Journal of Information Systems* 22(3):295–316.

Donath, Judith, Karrie Karahalios, and Fernanda Viegas. 1999. "Visualizing Conversation." *Journal of Computer-Mediated Communication* 4(4):0–0.

Edwards, Jeffrey R. and Richard P. Bagozzi. 2000. "On the Nature and Direction of Relationships Between Constructs and Measures." *Psychological Methods* 5(2):155–174.

Eisenberg, Eric M. and Marsha G. Witten. 1987. "Reconsidering Openness in Organizational Communication." *Academy of Management Review* 12(3):418–426.

Fahrmeir, Ludwig, Christian Heumann, Rita Künstler, Iris Pigeot, and Gerhard Tutz. 2016. *Statistik: Der Weg Zur Datenanalyse*. 8th ed. Berlin, Germany: Springer Spektrum.

Fang, Yulin et al. 2014. "Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-Commerce Institutional Mechanisms." *MIS Quarterly* 38(2):407–427.

Fecheyr-Lippens, Bruce, Bill Schaninger, and Karen Tanner. 2015. "Power to the New People Analytics." *McKinsey & Company*. Retrieved January 2, 2017 (http://www.mckinsey.com/ business-functions/organization/our-insights/power-to-the-new-people-analytics).

Fisher, Robert J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning." *Journal of Consumer Research* 20(2):303–315.

Galford, Robert and Anne Drapeau. 2003. "The Enemies of Trust." *Harvard Business Review* 81(2):88–95.

Gefen, David, Detmar W. Straub, and Marie-Claude Boudreau. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice." *Communications of the Association for Information Systems* 4(7):2–76.

Gerlach, Jin, Thomas Widjaja, and Peter Buxmann. 2015. "Handle with Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior." *The Journal of Strategic Information Systems* 24(1):33–43.

Gibbs, Jennifer L., Nik Ahmad Rozaidi, and Julia Eisenberg. 2013. "Overcoming the 'Ideology of Openness': Probing the Affordances of Social Media for Organizational Knowledge Sharing." *Journal of Computer-Mediated Communication* 19(1):102–120.

Gross, Ralph and Alessandro Acquisti. 2005. "Information Revelation and Privacy in Online Social Networks." in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*.

Grudin, Jonathan. 2006. "Enterprise Knowledge Management and Emerging Technologies." in *Proceedings of the 39th Annual Hawaii International Conference on System Science*.

Hacker, Janine, Freimut Bodendorf, and Pascal Lorenz. 2016. "A Framework to Analyze Enterprise Social Network Data." Pp. 84–107 in *Enterprise Big Data Engineering, Analytics, and Management*, edited by M. Atzmueller, S. Oussena, and T. Roth-Berghofer. IGI Global.

Haenlein, Michael and Andreas M. Kaplan. 2004. "A Beginner's Guide to Partial Least Squares Analysis." *Understanding Statistics* 3(4):283–297.

Hair, Jospeh F., William C. Black, Barry J. Babin, and Rolph E. Anderson. 2006. *Multivariate Data Analysis*. 6th ed. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Herrmann, Andreas, Christian Homburg, and Martin Klarmann. 2008. "Strukturgleichungsmodelle Mit Latenten Variablen: Kausalanalyse." in *Handbuch Marktforschung: Methoden – Anwendungen – Praxisbeispiele*, edited by A. Hermann, C. Homburg, and M. Klarmann. Wiesbaden, Germany: Gabler.

Herzog, Christian, Alexander Richter, Melanie Steinhueser, Uwe Hoppe, and Michael Koch. 2013. "Methods and Metrics for Measuring the Success of Enterprise Social Software – What We Can Learn From Practice and Vice Versa." in *Proceedings of the 21st European Conference on Information Systems*.

Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta. 1999. "Building Consumer Trust Online." *Communications of the ACM* 42(4):80–85.

Hollenbaugh, Erin E. and Amber L. Ferris. 2014. "Facebook Self-Disclosure: Examining the Role of Traits, Social Cohesion, and Motives." *Computers in Human Behavior* 30:50–58.

Homans, George C. 1958. "Social Behavior as Exchange." *American Journal of Sociology* 63(6):597–606.

Homburg, Christian and Annette Giering. 1996. "Konzeptualisierung Und Operationalisierung Komplexer Konstrukte: Ein Leitfaden Für Die Marketingforschung." *Marketing: Zeitschrift Für Forschung Und Praxis* 18(1):5–24.

Homburg, Christian and Martin Klarmann. 2006. "Die Kausalanalyse in Der Empirischen Betriebswirtschaftlichen Forschung - Problemfelder Und Anwendungsempfehlungen - ProQuest." *Die Betriebswirtschaft* 66(6):727–748.

Hu, Li-tze and Peter M. Bentler. 1998. "Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification." *Psychological Methods* 3(4):424–453.

Hu, Li-tze and Peter M. Bentler. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives." *Structural Equation Modeling: A Multidisciplinary Journal* 6(1):1–55.

Hui, Kai-Lung, Hock-Hai Teo, and Sang-Yong Tom Lee. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment." *MIS Quarterly* 31(1):19–33.

Hurbean, Luminita and Doina Fotache. 2013. "Mobile Technology: Binding Social and Cloud

Into a New Enterprise Applications Platform." *Informatica Economica* 17(2):73–83.

Jackson, Anne, JoAnne Yates, and Wanda Orlikowski. 2007. "Corporate Blogging: Building Community Through Persistent Digital Talk." in *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Jarvis, Cheryl B., Scott B. MacKenzie, and Philip M. Podsakoff. 2004. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research." *Journal of Consumer Research* 30(2):199–218.

John, Oliver P., Eileen M. Donahue, and Robert L. Kentle. 1991. *The Big Five Inventory - Versions 4a and 54*. Berkeley, California: University of California, Institute of Personality and Social Research.

Johnson-Page, Grace F. and R.Scott Thatcher. 2002. "B2C Data Privacy Policies : Current Trends." *Management Decision* 39(4):262–271.

Junglas, Iris A. and Richard T. Watson. 2008. "Location-Based Services." *Communications of the ACM* 51(3):65–69.

Kim, Dan J., Donald L. Ferrin, and H.Raghav Rao. 2008. "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents." *Decision Support Systems* 44(2):544–564.

Kim, Won, Ok-Ran Jeong, and Sang-Won Lee. 2010. "On Social Web Sites." *Information Systems* 35(2):215–236.

Klein, Heinz K. and Michael D. Myers. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems." *MIS Quarterly* 23(1):67–93.

Kluemper, Donald H. and Peter A. Rosen. 2009. "Future Employment Selection Methods: Evaluating Social Networking Web Sites." *Journal of Managerial Psychology* 24(6):567–580.

Koch, Hope, Ester Gonzalez, and Dorothy Leidner. 2012. "Bridging the Work/Social Divide: The Emotional Response to Organizational Social Networking Sites." *European Journal of Information Systems* 21(6):699–717.

Koch, Hope, Dorothy Leidner, and Ester Gonzalez. 2013. "Digitally Enabling Social Networks: Resolving IT-Culture Conflict." *Information Systems Journal* 23(6):501–523.

Koroleva, Ksenia, Franziska Brecht, Luise Goebel, and Monika Malinova. 2011. " 'Generation Facebook' - A Cognitive Calculus Model of Teenage User Behavior on Social Network Sites." in *Proceedings of the 17th Americas Conference on Information Systems*.

Krasnova, Hanna, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. "Online Social Networks: Why We Disclose." *Journal of Information Technology* 25(2):109–125.

Krasnova, Hanna and Natasha F. Veltri. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA." in *Proceedings of the 43rd Annual Hawaii International Conference on System Sciences*.

Krasnova, Hanna, Natasha F. Veltri, and Oliver Günther. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture Intercultural Dynamics of Privacy Calculus." *Business and Information Systems Engineering* 4(3):127–135.

Kügler, Maurice, Sven Dittes, Stefan Smolnik, and Alexander Richter. 2015. "Connect Me! Antecedents and Impact of Social Connectedness in Enterprise Social Software." *Business & Information Systems Engineering* 57(3):181–196.

Kügler, Maurice and Stefan Smolnik. 2013. “Just for the Fun of It? Towards a Model for Assessing the Individual Benefits of Employees’ Enterprise Social Software Usage.” in *Proceedings of the 46th Hawaii International Conference on System Sciences*.

Kügler, Maurice and Stefan Smolnik. 2014. “Uncovering the Phenomenon of Employees' Enterprise Social Software Use in the Post- Acceptance Stage - Proposing a Use Typology.” in *Proceedings of the 22nd European Conference on Information Systems*.

Kügler, Maurice, Stefan Smolnik, and Gerald Kane. 2015. “What’s in IT for Employees? Understanding the Relationship between Use and Performance in Enterprise Social Software.” *The Journal of Strategic Information Systems* 24(2):90–112.

Kügler, Maurice, Stefan Smolnik, and Philip Raeth. 2012. “Why Don’t You Use It? Assessing the Determinants of Enterprise Social Software Usage: A Conceptual Model Integrating Innovation Diffusion and Social Capital Theories.” in *Proceedings of the 33rd International Conference on Information Systems*.

Kwak, Haewoon, Changhyun Lee, Hosung Park, and Sue Moon. 2010. “What Is Twitter , a Social Network or a News Media?” in *Proceedings of the 19th International Conference on World Wide Web*.

Lapointe, Liette and Suzanne Rivard. 2005. “A Multilevel Model of Resistance to Information Technology Implementation.” *MIS Quarterly* 29(3):461–491.

LaRose, Robert and Nora J. Rifon. 2007. “Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior.” *Journal of Consumer Affairs* 41(1):127–149.

Larosiliere, Gregory and Dorothy Leidner. 2012. “The Effects of Social Network Usage on Organizational Identification.” in *Proceedings of the 33rd International Conference on Information Systems*.

Laufer, Robert S. and Maxine Wolfe. 1977. “Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory.” *Journal of Social Issues* 33(3):22–42.

Leidner, Dorothy, Hope Koch, and Ester Gonzalez. 2010. “Assimilating Generation Y IT New Hires into USAA’s Workforce: The Role of an Enterprise 2.0 System.” *MIS Quarterly Executive* 9(4):229–242.

Leonardi, Paul M. 2011. “Innovation Blindness: Culture, Frames, and Cross-Boundary Problem Construction in the Development of New Technology Concepts.” *Organization Science* 22(2):347–369.

Leonardi, Paul M., Marleen Huysman, and Charles Steinfield. 2013. “Enterprise Social Media: Definition, History, and Prospects for the Study of Social Technologies in Organizations.” *Journal of Computer-Mediated Communication* 19(1):1–19.

Li, Han and Rathindra Sarathy. 2007. “Understanding Online Information Disclosure as a Privacy Calculus Adjusted by Exchange Fairness.” in *Proceedings of the 28th International Conference on Information Systems*.

Li, Han, Rathindra Sarathy, and Heng Xu. 2010. “Understanding Situational Online Information Disclosure as a Privacy Calculus.” *Journal of Computer Information Systems* 51(1):62–71.

Li, Han, Rathindra Sarathy, and Heng Xu. 2011. “The Role of Affect and Cognition on Online Consumers’ Decision to Disclose Personal Information to Unfamiliar Online Vendors.” *Decision Support Systems* 51(3):434–445.

Li, Yuan. 2011. “Empirical Studies on Online Information Privacy Concerns : Literature Review and an Integrative Framework.” *Communications of the Association for Information Systems* 28(28):453–496.

Liang, Huigang, Nilesh Saraf, Qing Hu, and Yajiong Xue. 2014. “Assimilation of Enterprise Systems - The Effect of Institutional Pressures and the Mediating Role of Top Management.” *MIS Quarterly* 31(1):59–87.

Liao, Chechen, Chuang-Chun Liu, and Kuanchin Chen. 2011. “Examining the Impact of Privacy, Trust and Risk Perceptions Beyond Monetary Transactions: An Integrated Model.” *Electronic Commerce Research and Applications* 10(6):702–715.

Lin, Angela and Leiser Silva. 2005. “The Social and Political Construction of Technological Frames.” *European Journal of Information Systems* 14(1):49–59.

Lowry, Paul B. and James Gaskin. 2014. “Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It.” *IEEE Transactions on Professional Communication* 57(2):123–146.

Lowry, Paul B. and Gregory D. Moody. 2015. “Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies.” *Information Systems Journal* 25(5):433–463.

MacKenzie, Scott B., Philip M. Podsakoff, and Nathan P. Podsakoff. 2011. “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques.” *MIS Quarterly* 35(2):293–334.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” *Information Systems Research* 15(4):336–355.

Markus, M.Lynne. 1983. “Power, Politics, and MIS Implementation.” *Communications of the ACM* 23(6):430–444.

Mattox, Dave, Mark Maybury, and Daryl Morey. 1999. “Enterprise Expert and Knowledge Discovery.” in *Proceedings of the 8th International Conference on Human-Computer Interaction*.

Mazmanian, Melissa. 2013. “Avoiding the Trap of Constant Connectivity: When Congruent Frames Allow for Heterogeneous Practices.” *Academy of Management Journal* 56(5):1225–1250.

McAfee, Andrew P. 2006. “Enterprise 2.0: The Dawn of Emergent Collaboration.” *MIT Sloan Management Review* 47(3):21–28.

McAfee, Andrew P. 2011. “Shattering the Myths About Enterprise 2.0 Andrew.” *Center for Digital Business - Research Brief* 13(1):1–6.

McAfee, Andrew P. 2013. *Enterprise 2.0: How to Manage Social Technologies to Transform Your Organization*. Boston, Massachusetts: Harvard Business Press.

McGovern, Tom and Christian Hicks. 2004. “How Political Processes Shaped the IT Adopted by a Small Make-to-Order Company: A Case Study in the Insulated Wire and Cable Industry.” *Information and Management* 42(1):243–257.

McKnight, D.Harrison, Vivek Choudhury, and Charles Kacmar. 2002. “Developing and Validating Trust Measures for E-Commerce: An Integrative Typology.” *Information Systems Research* 13(3):334–359.

Metzger, Miriam J. 2004. “Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce.” *Journal of Computer-Mediated Communication* 9(4). Retrieved April 25, 2016 (http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2004.tb00292.x/full).

Milberg, Sandra J., H.Jeff Smith, and Sandra J. Burke. 2000. “Information Privacy: Corporate Management and National Regulation.” *Organization Science* 11(1):35–57.

Milne, George R. and Maria-Eugenia Boza. 1999. “Trust and Concern in Consumers’ Perception of Marketing Information Management Practices.” *Journal of Interactive Marketing* 13(1):5–24.

Mishra, Abhay Nath and Ritu Agarwal. 2010. “Technological Frames, Organizational Capabilities, and IT Use: An Empirical Investigation of Electronic Procurement.” *Information Systems Research* 21(2):249–270.

Mokbel, Mohamed F., Chin-Yin Chow, and Walid G. Aref. 2007. “The New Casper: A Privacy-Aware Location-Based Database Server.” in *Proceedings of the 23rd International Conference in Data Engineering*.

Momin, Weena Yancey M. and Kushendra Mishra. 2015. “HR Analytics as a Strategic Workforce Planning.” *International Journal of Advanced Research* 1(4):258–260.

Moon, Youngme. 2000. “Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers.” *Journal of Consumer Research* 26(4):323–339.

Moon, Youngme. 2003. “Don’t Blame the Computer: When Self-Disclosure Moderates the Self-Serving Bias.” *Journal of Consumer Psychology* 13(1–2):125–137.

Morrison, Elizabeth W. and Sandra L. Robinson. 1997. “When Employees Feel Betrayed: A Model of How Psychological Contract Violation Develops.” *Academy of Management Review* 22(1):226–256.

Myers, Michael D. and Michael Newman. 2007. “The Qualitative Interview in IS Research: Examining the Craft.” *Information and Organization* 17(1):2–26.

O’Mahony, Siobhan and Stephen R. Barley. 1999. “Do Digital Telecommunications Affect Work and Organization? The State of Our Knowledge.” Pp. 125–161 in *Research in Organizational Behavior*, vol. 21. Greenwich, Connecticut: JAI Press.

Okazaki, Shintaro, Hairong Li, and Morikazu Hirose. 2009. “Consumer Privacy Concerns and Preference for Degree of Regulatory Control.” *Journal of Advertising* 38(4):63–77.

Olesen, Karin. 2014. “Implications of Dominant Technological Frames Over a Longitudinal Period.” *Information Systems Journal* 24(3):207–228.

Orlikowski, Wanda J. and Debra C. Gash. 1994. “Technological Frames: Making Sense of Information Technology in Organizations.” *ACM Transactions on Information Systems* 12(2):174–207.

Pavlou, Paul A. and David Gefen. 2004. “Building Effective Online Marketplaces with Institution-Based Trust.” *Information Systems Research* 15(1):37–59.

Pavlou, Paul A. and David Gefen. 2005. “Psychological Contract Violation in Online Marketplaces: Antecedents , Consequences , and Moderating Role.” *Information Systems Research* 16(4):372–399.

Pavlou, Paul A., Huigang Liang, and Yajiong Xue. 2007. “Understanding and Mitigating Uncertainty in Online Environments: A Principal-Agent Perspective.” *MIS Quarterly* 31(1):105–136.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. “Privacy Concerns and Consumer Willingness to Provide Personal Information.” *Journal of Public Policy & Marketing* 19(1):27–41.

Phillips, Lynn W. 1981. “Key Reports: A Methodological Organizational Analysis Marketing Measurement.” *Journal of Marketing Research* 18(4):395–415.

Podsakoff, Philip M., Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.” *The Journal of Applied Psychology* 88(5):879–903.

Podsakoff, Philip M., Scott B. MacKenzie, and Nathan P. Podsakoff. 2012. “Sources of Method Bias in Social Science Research and Recommendations on How to Control It.” *Annual Review of Psychology* 63:539–569.

Posey, Clay, Rebecca J. Bennett, Tom L. Roberts, and Paul Benjamin Lowry. 2011. “When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse.” *Journal of Information System Security* 7(1):24–47.

Posey, Clay, Paul Benjamin Lowry, Tom L. Roberts, and T.Selwyn Ellis. 2010. “Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the U.K. Who Use Online Communities.” *European Journal of Information Systems* 19(2):181–195.

Preacher, Kristopher J. and Andrew F. Hayes. 2004. “SPSS and SAS Procedures for Estimating Indirect Effects in Simple Mediation Models.” *Behavior Research Methods, Instruments & Computers* 36(4):717–731.

Raeth, Philip, Maurice Kügler, and Stefan Smolnik. 2011. “Measuring the Impact of Organizational Social Web Site Usage on Work Performance: A Multilevel Model.” in *Proceedings of the 32nd International Conference on Information Systems*.

Restubog, Simon L. D., Thomas J. Zagenczyk, Prashant Bordia, and Robert L. Tang. 2013. “When Employees Behave Badly: The Roles of Contract Importance and Workplace Familism in Predicting Negative Reactions to Psychological Contract Breach.” *Journal of Applied Social Psychology* 43(3):673–686.

Richter, Alexander and Kai Riemer. 2009. “Corporate Social Networking Sites – Modes of Use and Appropriation through Co-Evolution.” in *Proceedings of the 20th Australasian Conference on Information Systems*.

Richter, Daniel, Kai Riemer, and Jan vom Brocke. 2011. “Internet Social Networking - Stand Der Forschung Und Konsequenzen Für Enterprise 2.0.” *Business & Information Systems Engineering* 3(2):89–101.

Ring, Peter S. and Andrew H. Van de Ven. 1994. “Developmental Processes of Cooperative Interorganizational Relationships.” *Academy of Management Review* 19(1):90–118.

Robinson, Sandra L. 1996. “Trust and Breach of the Psychological Contract.” *Administrative Science Quarterly* 41(4):574–599.

Robinson, Sandra L. and Elizabeth W. Morrison. 2000. “The Development of Psychological Contract Breach and Violation: A Longitudinal Study.” *Journal of Organizational Behavior* 21(5):525–546.

Robinson, Sandra L. and Denise M. Rousseau. 1994. “Violating the Psychological Contract: Not the Exception but the Norm.” *Journal of Organizational Behavior* 15(3):245–259.

Romrée, Henri de, Bruce Fecheyr-Lippens, and Bill Schaninger. 2016. “People Analytics Reveals Three Things HR May Be Getting Wrong.” *McKinsey & Company*. Retrieved January 2, 2017 (http://www.mckinsey.com/business-functions/organization/our-insights/people-analytics-reveals-three-things-hr-may-be-getting-wrong).

Rousseau, Denise M. 1989. “Psychological and Implied Contracts in Organizations.” *Employee Responsibilities and Rights Journal* 2(2):121–139.

Rousseau, Denise M. and Judi McLean Parks. 1993. “The Contracts of Individuals and Organizations.” Pp. 1–47 in *Research in Organizational Behavior*, vol. 15. Greenwich, Connecticut: JAI Press.

Sarker, Suprateek, Xiao Xiao, and Tanya Beaulieu. 2013. “Qualitative Studies in Information Systems : A Critical Review and Some Guiding Principles.” *MIS Quarterly* 37(4):Guest Editorial.

Schäffer, Utz. 2007. *Management Accounting & Control Scales Handbook*. Wiesbaden, Germany: Springer Science & Business Media.

Schoenbachler, Denise D. and Geoffrey L. Gordon. 2002. “Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing.” *Journal of Interactive Marketing* 16(3):2–16.

Schöndienst, Valentin, Hanna Krasnova, Oliver Günther, and Dirk Riehle. 2011. “Micro-Blogging Adoption in the Enterprise: An Empirical Analysis.” in *Proceedings of the 10th International Conference on Wirtschaftsinformatik*.

Sewell, Graham and James R. Barker. 2006. “Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance.” *Academy of Management Review* 31(4):934–961.

Shaw, Nancy C. and James S. K. Ang. 1994. “Understanding End-User Computing through Technological Frames.” in *Proceedings of the 18th International Conference on Information Systems*.

Sipior, Janice C., Burke T. Ward, and Regina Connolly. 2013. “Privacy in Online Social Networking: Applying a Privacy Calculus Model.” in *Proceedings of the 17th Pacific Asia Conference on Information Systems*.

Smith, H.Jeff. 2001. “Information Privacy and Marketing: What the U.S. Should (and Shouldn’t) Learn from Europe.” *California Management Review* 43(2):8–33.

Smith, H. Jeff, Tamara Dinev, and Heng Xu. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35(4):989–1015.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices.” *MIS Quarterly* 20(2):167–196.

Son, Jai-Yeol and Sung S. Kim. 2008. “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model.” *MIS Quarterly* 32(3):503–529.

Stanton, Jeffrey M. and Kathryn R. Stam. 2003. “Information Technology, Privacy, and Power within Organizations: A View from Boundary Theory and Social Exchange Perspectives.” *Surveillance & Society* 1(2):152–190.

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner, and Stephen McClure. 1983. “A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations.” *Journal of Applied Psychology* 68(3):459–468.

Taddei, Stefano and Bastianina Contena. 2013. “Privacy, Trust and Control: Which Relationships

with Online Self-Disclosure?" *Computers in Human Behavior* 29(3):821–826.

Treem, Jeffrey W. and Paul M. Leonardi. 2013. "Social Media Use in Organizations: Exploring the Affordances of Visibility, Editablity, Persistence, and Association." *Annals of the International Communication Association* 36(1):143–189.

Urbach, Nils and Frederik Ahlemann. 2010. "Structural Equation Modeling in Information Systems Research Using Partial Least Squares." *Journal of Information Technology Theory and Application* 11(2):5–40.

De Vaus, David. 2002. *Surveys in Social Research*. 5th ed. Abingdon, Oxon: Routledge.

De Vaus, David. 2014. *Surveys In Social Research*. 6th ed. Abingdon, Oxon: Routledge.

Veltri, Natasha F., Hanna Krasnova, and Wafa Elgarah. 2011. "Online Disclosure and Privacy Concerns: A Study of Moroccan and American Facebook Users." in *Proceedings of the 17th Americas Conference on Information Systems*.

Venkatesh, Viswanath and Hillol Bala. 2008. "Technology Acceptance Model 3 and a Research Agenda on Interventions." *Decision Sciences* 39(2):273–315.

Venkatesh, Viswanath, Susan A. Brown, and Hillol Bala. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems." *Management of Information Systems Quarterly* 37(3):855–879.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27(3):425–478.

Venkatraman, N. and John Grant. 1986. "Construct Measurement in Organizational Strategy Research: A Critique and Proposal." *Academy of Management Review* 11(1):71–87.

Wakefield, Robin. 2013. "The Influence of User Affect in Online Information Disclosure." *Journal of Strategic Information Systems* 22(2):157–174.

Walker, Helen M. 1940. "Degrees of Freedom." *Journal of Educational Psychology* 31(4):253–269.

Walsham, Geoff. 2006. "Doing Interpretive Research." *European Journal of Information Systems* 15(3):320–30.

Walsham, Geoff. 2013. "Empiricism in Interpretive IS Research: A Response to Stahl." *European Journal of Information Systems* 23(1):12–16.

Wattal, Sunil, Pradeep Racherla, and Munir Mandviwalla. 2010. "Network Externalities and Technology Use: A Quantitative Analysis of Intraorganizational Blogs." *Journal of Management Information Systems* 27(1):145–174.

Webb, Thomas L. and Paschal Sheeran. 2006. "Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence." *Psychological Bulletin* 132(2):249–268.

Weible, Ricky Jay. 1993. *Privacy and Data: An Empirical Study of the Influence of Types of Data and Situational Context Upon Privacy Perceptions*. Mississippi State: Mississippi State University.

Weick, Karl E. 1979. "Cognitive Processes in Organizations." *Research in Organizational Behavior* 1(1):41–74.

Wellman, Barry, Janet Salaff, Dimitrina Dimitrova, Milena Gulia, and Caroline Haythornthwaite. 1996. “Computer Networks as Social Networks: Collaborative Work , Telework , and Virtual Community.” Pp. 213–238 in *Annual Review of Sociology*, vol. 22.

Westin, Alan F. 1967. *Privacy and Freedom*. New York, NY.

Westin, Alan F. 2003. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59(2):431–453.

White, Tiffany Barnett. 2004. “Consumer Disclosure and Disclosure Avoidance: A Motivational Framework.” *Journal of Consumer Psychology* 14(1–2):41–51.

Wilson, David W. and Joseph S. Valacich. 2012. “Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus.” in *Proceedings of the 33rd International Conference on Information Systems*.

Xu, Heng, Tamara Dinev, H.Jeff Smith, and Paul Hart. 2008. “Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View.” in *Proceedings of the 29th International Conference on Information Systems*.

Xu, Heng, Tamara Dinev, H.Jeff Smith, and Paul Hart. 2011. “Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances.” *Journal of the Association for Information Systems* 12(12):798–824.

Xu, Heng, Hock-Hai Teo, and Bernard C. Y. Tan. 2005. “Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk.” in *Proceedings of the 26th International Conference on Information Systems*.

Xu, Heng, Hock-Hai Teo, Bernard C. Y. Tan, and Ritu Agarwal. 2010. “The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services.” *Journal of Management Information Systems* 26(3):135–174.

Yang, Shu and Kanliang Wang. 2009. “The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention.” *ACM SIGMIS Database* 40(1):38–51.

Yimam-Seid, Dawit and Alfred Kobsa. 2003. “Expert-Finding Systems for Organizations: Problem and Domain Analysis and the DEMOIR Approach.” *Journal of Organizational Computing and Electronic Commerce* 13(1):1–24.

Yin, Robert K. 2011. *Applications of Case Study Research*. 3rd ed. Thousand Oaks, California: Sage Publications.

Yoshioka, Takeshi, JoAnne Yates, and Wanda Orlikowski. 2002. “Community-Based Interpretive Schemes: Exploring the Use of Cyber Meetings within a Global Organization.” in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*.

Zhao, Hao, Sandy J. Wayne, Brian C. Glibkowski, and Jesus Bravo. 2007. “The Impact of Psychological Contract Breach on Work Related Outcomes: A Meta Analysis.” *Personnel Psychology* 60(3):647–680.

Zhao, Xinshu, John G. Lynch Jr., and Qimei Chen. 2010. “Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis.” *Journal of Consumer Research* 37(2):197–206.

Appendix A – Survey Questions

Construct	Question	
Sensitivity of Information (Based on Dinev et al. 2013)	SI1	I do not feel comfortable with the type of information the system requests from me.
	SI2	I feel that the system requests highly sensitive information about me.
	SI3	The information I provide to the system is very sensitive to me.
Perceived Control (Based on Xu et al. 2011)	PC1	I believe I have control over who can get access to my information requested by the system.
	PC2	I think I have control over what information is released by the system.
	PC3	I believe I have control over how information is used by the system.
	PC4	I believe I can control my information provided to the system.
Perceived Information-Based Vulnerability (PIBV) (self-developed items, partially based on Dinev and Hart 2004)	PIBV1	Submitted information could be misused.
	PIBV2	Submitted information could be made available to unknown individuals in my company without my knowledge.
	PIBV3	Submitted information could be inappropriately used.
	PIBV4	Submitted information could be used to my disadvantage. **(rejected)**
	PIBV5	It might be beneficial for my company to use submitted information without considering my interests.
	PIBV6	Submitted information could be used for unfavorable personal decisions. **(rejected)**
	PIBV7	Submitted information could be exploited by the company.
Psychological Contract Breach (Based on Robinson & Morrison 2000)	PCB1	Almost all the promises made by my employer during recruitment have been kept so far (reverse).
	PCB2	I feel that my employer has come through in fulfilling the promises made to me when I was hired (reverse).
	PCB3	So far my employer has done an excellent job of fulfilling its promises to me (reverse).
	PCB4	I have not received everything promised to me in exchange for my contributions.
	PCB5	My employer has broken many of its promises to me even though I've upheld my side of the deal.
Psychological Contract Violation (Based on Robinson & Morrison 2000)	PCV1	I feel a great deal of anger toward my organization.
	PCV2	I feel betrayed by my organization.
	PCV3	I feel that my organization has violated the contract between us.
	PCV4	I feel extremely frustrated by how I have been treated by my organization.

Construct	Question	
Trust into Employer (Based on Robinson and Rousseau 1994)	T1	I am not sure I fully trust my employer (reversed)
	T2	My employer is open and upfront with me.
	T3	I believe my employer has high integrity.
	T4	In general, I believe my employer‘s motives and intentions are good.
	T5	My employer is not always honest and truthful (reversed).
	T6	I don‘t think my employer treats me fairly (reversed).
	T7	I can expect my employer to treat me in a consistent and predictable fashion.
Perceived Benefits (Based on Kim et al. 2008)	B1	Revealing my information in the system helps me to obtain advantages.
	B2	I need to provide my information so I can get exactly what I want from the system.
	B3	I believe that as a result of my information disclosure in the system, I can benefit from a better, customized service.
Intention to Disclose (Based on Xu et al. 2010)	ID1	Please specify the extent to which you would be willing to reveal your information in the system.
	ID2	How probable would it be that you would disclose information in the system?
	ID3	Would you disclose your information in the system?
Apathy (Based on Lapointe and Rivard’s (2005) developed resistance levels)	AP1	I feel indifferent towards the system
	AP2	I don’t care about the system
	AP3	I am not interested into the system
Passive Resistance (Based on Lapointe and Rivard’s (2005) developed resistance levels)	PR1	I disagree with the implementation of the system.
	PR2	I perceive the system as a negative change.
	PR3	I have a negative attitude towards the system.
Active Resistance (Based on Lapointe and Rivard’s (2005) developed resistance levels)	AR1	I will ask others not to use the system.
	AR2	I will reject the system.
	AR3	I will point out my negative view regarding the system to others.

Appendix B – R Code of Covariance Analysis

```
————————# Install and Initialize Necessary Packages
install.packages("car")
install.packages("foreign")
install.packages("lavaan")
install.packages("psy")
install.packages("psych")
install.packages("semPlot")
install.packages("qgraph")

library("car")
library("foreign")
library("lavaan")
library("psy")
library("psych")
library("semPlot")
library("qgraph")


————————# Data Import
Daten                       <-read.csv (file="PATH_TO_CSV.csv", header=TRUE, sep=";", dec=".",
na.strings="-77")


————————# Structural Equation Model of PIBV
 sem.PIBV.model             <- '

# measurement model
InfoSensitivity             =~ SI_1+SI_2+SI_3
Control                     =~ PC_1+PC_2+ PC_3+ PC_4
ContractBreach              =~ CB_1+ CB_2+ CB_3+ CB_4+ CB_5
ContractViolation           =~ CV_1+ CV_2+ CV_3+ CV_4
Trust                       =~ T_1+ T_2+ T_3+ T_4+ T_5+ T_6+ T_7
PIBV                        =~ PIBV_1+ PIBV_2+ PIBV_3+ PIBV_4+ PIBV_5
Benefit                     =~ B_1+ B_2+ B_3
Disclosure                  =~ ID_1+ ID_2+ ID_3
Apathy                      =~ AP_1+ AP_2+ AP_3
Passive.Res                 =~ PR_1+ PR_2+ PR_3
Active.Res                  =~ AR_1+ AR_2+ AR_3

# regressions
Trust                       ~ ContractViolation + ContractBreach
ContractViolation           ~ ContractBreach
PIBV                        ~ InfoSensitivity + Control + ContractViolation + ContractBreach + Trust
Disclosure                  ~ PIBV + Benefit
Apathy                      ~ PIBV + Benefit
Passive.Res                 ~ PIBV + Benefit
Active.Res                  ~ PIBV + Benefit'


————————# Insert Data into Model & Show Summary
sem.PIBV                    <- sem(sem.PIBV.model, data=Daten)
summary(sem.PIBV)


————————# Testing for Mediation of Trust into Employer for Psychological Contract Violation
sem.PIBVMediationCV.model <- '

# measurement model
InfoSensitivity             =~ SI_1+SI_2+SI_3
Control                     =~ PC_1+PC_2+ PC_3+ PC_4
ContractBreach              =~ CB_1+ CB_2+ CB_3+ CB_4+ CB_5
ContractViolation           =~ CV_1+ CV_2+ CV_3+ CV_4
```

```
Trust                    =~ T_1+ T_2+ T_3+ T_4+ T_5+ T_6+ T_7
PIBV                     =~ PIBV_1+ PIBV_2+ PIBV_3+ PIBV_4+ PIBV_5
Benefit                  =~ B_1+ B_2+ B_3
Disclosure               =~ ID_1+ ID_2+ ID_3
Apathy                   =~ AP_1+ AP_2+ AP_3
Passive.Res              =~ PR_1+ PR_2+ PR_3
Active.Res               =~ AR_1+ AR_2+ AR_3

# regressions
Trust                    ~ a*ContractViolation
ContractViolation        ~ ContractBreach
PIBV                     ~  InfoSensitivity + Control + c*ContractViolation + ContractBreach +
e*Trust
Disclosure               ~ PIBV + Benefit
Apathy                   ~ PIBV + Benefit
Passive.Res              ~ PIBV + Benefit
Active.Res               ~ PIBV + Benefit

indirect                 := a*e
direct                   := c
total                    := c + (a*e)'

——# Insert Data into Model & Show Summary
sem.PIBVMediationCV <- sem(sem.PIBVMediationCV.model, data = Daten)
summary(sem.PIBVMediationCV)

——# Conduct Bootstrap Analysis
boot.fit.CV              <- parameterEstimates(sem.PIBVMediationCV,
                         boot.ci.type="bca.simple",level=0.95, ci=TRUE,standardized = FALSE)
boot.fit.CV


————————# Testing for Mediation of Trust into Employer for Psychological Contract Breach
 sem.PIBVMediationCB.model <- '
# measurement model
InfoSensitivity          =~ SI_1+SI_2+SI_3
Control                  =~ PC_1+PC_2+ PC_3+ PC_4
ContractBreach           =~ CB_1+ CB_2+ CB_3+ CB_4+ CB_5
ContractViolation        =~ CV_1+ CV_2+ CV_3+ CV_4
Trust                    =~ T_1+ T_2+ T_3+ T_4+ T_5+ T_6+ T_7
PIBV                     =~ PIBV_1+ PIBV_2+ PIBV_3+ PIBV_4+ PIBV_5
Benefit                  =~ B_1+ B_2+ B_3
Disclosure               =~ ID_1+ ID_2+ ID_3
Apathy                   =~ AP_1+ AP_2+ AP_3
Passive.Res              =~ PR_1+ PR_2+ PR_3
Active.Res               =~ AR_1+ AR_2+ AR_3

# regressions
Trust                    ~ b*ContractBreach
ContractViolation        ~ ContractBreach
PIBV                     ~  InfoSensitivity + Control + c*ContractViolation + d*ContractBreach +
e*Trust
Disclosure               ~ PIBV + Benefit
Apathy                   ~ PIBV + Benefit
Passive.Res              ~ PIBV + Benefit
Active.Res               ~ PIBV + Benefit

indirect                 := b*e
direct                   := d
total                    := d + (b*e)'

——# Insert Data into Model & Show Summary
sem.PIBVMediationCB <- sem(sem.PIBVMediationCB.model, data = Daten)
summary(sem.PIBVMediationCB)
```

```
----# Conduct Bootstrap Analysis
boot.fit.CB                    <- parameterEstimates(sem.PIBVMediationCB, boot.ci.type="bca.simple",
                                  level=0.95, ci=TRUE, standardized = FALSE)
boot.fit.CB


----------# Testing Global and Local Goodness-of-Fit #----------
----# Global Goodness-of-Fit (SRMR, RMSEA, NNFI, CFI)
fitMeasures(sem.PIBV)



----# Correlation Matrix of Latent Constructs
  lavInspect(sem.PIBV,'cor.lv')


----# Doing a CFA (confirmatory factor analysis)
PIBV                <- ('PIBV =~ PIBV_1+ PIBV_2+ PIBV_3+ PIBV_4+ PIBV_5')
cfa.PIBV            <- cfa(PIBV, data = Daten)
summary(cfa.PIBV)

Apathy              <- ('Apathy =~ AP_1+ AP_2+ AP_3')
cfa.Apathy          <- cfa(Apathy, data = Daten)
summary(cfa.Apathy)

Passive.Res         <- ('Passive.Res =~ PR_1+ PR_2+ PR_3')
cfa.Passive.Res     <- cfa(Passive.Res, data = Daten)
summary(cfa.Passive.Res)

Active.Res          <- ('Active.Res =~ AR_1+ AR_2+ AR_3')
cfa.Active.Res      <- cfa(Active.Res, data = Daten)
summary(cfa.Active.Res)


----# Measure R Square --> Indicator Reliability
lavInspect(cfa.PIBV,"rsquare")
lavInspect(cfa.Apathy,"rsquare")
lavInspect(cfa.Passive.Res,"rsquare")
lavInspect(cfa.Active.Res,"rsquare")


----# Measure AVE
AVE.PIBV            <- mean(lavInspect(cfa.PIBV,"rsquare"))
print(AVE.PIBV)

AVE.Apathy          <- mean(lavInspect(cfa.Apathy,"rsquare"))
print(AVE.Apathy)

AVE.Passive.Res     <- mean(lavInspect(cfa.Passive.Res,"rsquare"))
print(AVE.Passive.Res)

AVE.Active.Res      <- mean(lavInspect(cfa.Active.Res,"rsquare"))
print(AVE.Active.Res)


----# Measure Factor/Construct Reliability
CR.PIBV<-
(sum(lavInspect(cfa.PIBV,"standardized")$lambda))^2/((sum(lavInspect(cfa.PIBV,"standardized")$lambda))^2
+sum(lavInspect(cfa.PIBV,"standardized")$theta))
print(CR.PIBV)

CR.Apathy<-
(sum(lavInspect(cfa.Apathy,"standardized")$lambda))^2/((sum(lavInspect(cfa.Apathy,"standardized")$lambd
a))^2+sum(lavInspect(cfa.Apathy,"standardized")$theta))
```

```
print(CR.Apathy)

CR.Passive.Res<-
(sum(lavInspect(cfa.Passive.Res,"standardized")$lambda))^2/((sum(lavInspect(cfa.Passive.Res,"standardized")
$lambda))^2+sum(lavInspect(cfa.Passive.Res,"standardized")$theta))
print(CR.Passive.Res)

CR.Active.Res<-
(sum(lavInspect(cfa.Active.Res,"standardized")$lambda))^2/((sum(lavInspect(cfa.Active.Res,"standardized")$l
ambda))^2+sum(lavInspect(cfa.Active.Res,"standardized")$theta))
print(CR.Active.Res)


----# Measure Item-to-Total Correlation & Cronbach's Alpha
alpha.PIBV          <- alpha(data.frame(cbind(Daten$PIBV_1,Daten$ PIBV_2,Daten$ PIBV_3, Daten$
                    PIBV_4, Daten$ PIBV_5)))
names(alpha.PIBV)
alpha.PIBV$item.stats
alpha.PIBV$total

alpha.Apathy        <- alpha(data.frame(cbind(Daten$AP_1,Daten$ AP_2,Daten$ AP_3)))
names(alpha.Apathy)
alpha.Apathy$item.stats
alpha.Apathy$total

alpha.Passive.Res   <- alpha(data.frame(cbind(Daten$PR_1,Daten$PR_2,Daten$PR_3)))
names(alpha.Passive.Res)
alpha.Passive.Res$item.stats
alpha.Passive.Res$total

alpha.Active.Res    <- alpha(data.frame(cbind(Daten$AR_1,Daten$AR_2,Daten$AR_3)))
names(alpha.Active.Res)
alpha.Active.Res$item.stats
alpha.Active.Res$total


----------# Create a Matrix and then a Correlation Matrix
matrix.PIBV         <-cbind(Daten$PIBV_1,Daten$ PIBV_2,Daten$ PIBV_3,Daten$ PIBV_4, Daten$ PIBV_5)
matrix.PIBV         <- na.omit(matrix.PIBV)
round(cor(matrix.PIBV),2)

matrix.Apathy       <- cbind(Daten$AP_1,Daten$ AP_2,Daten$ AP_3)
matrix.Apathy       <- na.omit(matrix.Apathy)
round(cor(matrix.Apathy),2)

matrix.Passive.Res  <- cbind(Daten$PR_1,Daten$PR_2,Daten$PR_3)
matrix.Passive.Res  <- na.omit(matrix.Passive.Res)
round(cor(matrix.Passive.Res),2)

matrix.Active.Res   <- cbind(Daten$AR_1,Daten$AR_2,Daten$AR_3)
matrix.Active.Res   <- na.omit(matrix.Active.Res)
round(cor(matrix.Active.Res),2)

matrix.InfoSensitivity  <- cbind(Daten$SI_1,Daten$SI_2,Daten$SI_3)
matrix.InfoSensitivity  <- na.omit(matrix.InfoSensitivity)
round(cor(matrix.InfoSensitivity),2)

matrix.Control      <- cbind(Daten$PC_1,Daten$PC_2,Daten$PC_3,Daten$PC_4)
matrix.Control      <- na.omit(matrix.Control)
round(cor(matrix.Control),2)

matrix.ContractBreach  <- cbind(Daten$CB_1,Daten$CB_2,Daten$CB_3,Daten$CB_4,Daten$CB_5)
matrix. ContractBreach <- na.omit(matrix. ContractBreach)
round(cor(matrix. ContractBreach),2)
```

```
matrix.ContractViolation <- cbind(Daten$CV_1,Daten$CV_2,Daten$CV_3,Daten$CV_4)
matrix. ContractViolation <- na.omit(matrix. ContractViolation)
round(cor(matrix. ContractViolation),2)

matrix.Trust <-cbind(Daten$T_1,Daten$T_2,Daten$T_3,Daten$T_4, Daten$T_5,Daten$T_6,Daten$T_7)
matrix.Trust <- na.omit(matrix.Trust)
round(cor(matrix.Trust),2)

————————# Fornell-Larcker Criterion
 —#  1. Create Correlation Matrix
 —#  2. Take squares of the matrix
 —#  3. create AVE


————————# Standard Deviation & Mean of Latent Constructs
v.InfoSens              <- c(Daten$SI_1,Daten$SI_2,Daten$SI_3)
v.Disclosure                    <- c(Daten$v_39,Daten$v_40,Daten$v_41)
v.Benefit               <- c(Daten$v_32,Daten$v_33,Daten$v_34)
v.PIBV                          <- c(Daten$PIBV_1,Daten$ PIBV_2,Daten$ PIBV_3, Daten$ PIBV_4, Daten$
PIBV_5)
v.Trust                         <- c(Daten$T_1,Daten$T_2,Daten$T_3,Daten$T_4,
                                Daten$T_5,Daten$T_6,Daten$T_7)
v.ContractViolation     <- c(Daten$CV_1,Daten$CV_2,Daten$CV_3,Daten$CV_4)
v.ContractBreach                <- c(Daten$CB_1,Daten$CB_2,Daten$CB_3,Daten$CB_4,Daten$CB_5)
v.Control               <- c(Daten$PC_1,Daten$PC_2,Daten$PC_3,Daten$PC_4)
v.Passive.Res                   <- c(Daten$PR_1,Daten$PR_2,Daten$PR_3)
v.Active.Res                    <- c(Daten$AR_1,Daten$AR_2,Daten$AR_3)
v.Apathy                <- c(Daten$AP_1,Daten$ AP_2,Daten$ AP_3)

sd.Passive.Res                  <- sd(v.Passive.Res, na.rm=TRUE)
sd.Active.Res                   <- sd(v.Active.Res, na.rm=TRUE)
sd.Apathy               <- sd(v.Apathy, na.rm=TRUE)
sd.Disclosure                   <- sd(v.Disclosure, na.rm=TRUE)
sd.Benefit              <- sd(v.Benefit, na.rm=TRUE)
sd.PIBV                         <- sd(v.PIBV, na.rm=TRUE)
sd.Trust                        <- sd(v.Trust, na.rm=TRUE)
sd.ContractViolation    <- sd(v.ContractViolation, na.rm=TRUE)
sd.ContractBreach       <- sd(v.ContractBreach,na.rm=TRUE)
sd.Control              <- sd(v.Control, na.rm=TRUE)
sd.InfoSens                     <- sd(v.InfoSens, na.rm=TRUE)

mean.InfoSens                   <- mean(v.InfoSens, na.rm=TRUE)
mean.Control                    <- mean(v.Control, na.rm=TRUE)
mean.ContractBreach     <- mean(v.ContractBreach, na.rm=TRUE)
mean.ContractViolation          <- mean(v.ContractViolation, na.rm=TRUE)
mean.Trust                      <- mean(v.Trust, na.rm=TRUE)
mean.PIBV               <- mean(v.PIBV, na.rm=TRUE)
mean.Benefit                    <- mean(v.Benefit, na.rm=TRUE)
mean.Disclosure                 <- mean(v.Disclosure, na.rm=TRUE)
mean.Apathy                     <- mean(v.Apathy, na.rm=TRUE)
mean.Active.Res                 <- mean(v.Active.Res, na.rm=TRUE)
mean.Passive.Res                <- mean(v.Passive.Res, na.rm=TRUE)
```

Appendix C – Fornell-Larcker-Criterion Test

All matrices are based on the data set of Section 5 with $n=327$

	PIBV 1	PIBV 2	PIBV 3	PIBV 5	PIBV 7	AVE
PIBV 1	1					0.69
PIBV 2	0.55	1				0.69
PIBV 3	0.64	0.66	1			0.69
PIBV 5	0.35	0.24	0.36	1		0.69
PIBV 7	0.50	0.41	0.53	0.53	1	0.69

Fornell-Larcker Criterion Test: *Perceived Information-Based Vulnerability*

	AP 1	AP 2	AP 3	AVE
AP 1	1			0.62
AP 2	0.46	1		0.62
AP 3	0.26	0.37	1	0.62

Fornell-Larcker Criterion Test: *Apathy*

	PR 1	PR 2	PR 3	AVE
PR 1	1			0.87
PR 2	0.72	1		0.87
PR 3	0.72	0.79	1	0.87

Fornell-Larcker Criterion Test: *Passive Resistance*

	AR 1	AP 2	AP 3	AVE
AR 1	1			0.67
AR 2	0.46	1		0.67
AR 3	0.32	0.52	1	0.67

Fornell-Larcker Criterion Test: *Active Resistance*

Appendix D – Common Latent Factor Analysis

Construct	Indicator	Substantive Factor Loading (R1)	(R1)²	Method Factor Loading (R2)	(R2)²
Sensitivity of Information	SI1	0.65	0.42	-0.14	0.02
	SI2	0.9	0.81	-0.14	0.02
	SI3	0.79	0.62	-0.14	0.02
Perceived Control	PC1	0.86	0.74	-0.14	0.02
	PC2	0.92	0.85	-0.14	0.02
	PC3	0.87	0.76	-0.15	0.023
	PC4	0.86	0.74	-0.14	0.02
Psychological Contract Breach	PCB1	0.84	0.71	-0.17	0.029
	PCB2	0.94	0.88	-0.19	0.036
	PCB3	0.78	0.61	-0.16	0.026
	PCB4	0.55	0.3	-0.14	0.02
	PCB5	0.93	0.86	-0.17	0.029
Psychological Contract Violation	PCV1	0.78	0.61	-0.16	0.026
	PCV2	0.85	0.72	-0.24	0.058
	PCV3	0.89	0.79	-0.26	0.068
	PCV4	0.87	0.76	-0.24	0.058
Trust into Employer	T1	0.67	0.45	-0.15	0.023
	T2	0.86	0.74	-0.18	0.032
	T3	0.86	0.74	-0.19	0.036
	T4	0.71	0.5	-0.21	0.044
	T5	0.57	0.32	-0.15	0.023
	T6	0.53	0.28	-0.15	0.023
	T7	0.56	0.31	-0.17	0.029
PIBV	PIBV1	0.83	0.69	-0.17	0.029
	PIBV2	0.81	0.66	-0.16	0.026
	PIBV3	0.89	0.79	-0.17	0.029
	PIBV4	0.66	0.44	-0.16	0.026
	PIBV5	0.79	0.62	-0.17	0.029
Perceived Benefits	B1	0.69	0.48	-0.17	0.029
	B2	0.43	0.18	-0.17	0.029
	B3	0.75	0.56	-0.16	0.026
Intention to Disclose	ID1	0.86	0.74	-0.16	0.026
	ID2	0.94	0.88	-0.14	0.02
	ID3	0.93	0.86	-0.14	0.02
Apathy	AP1	0.75	0.56	-0.15	0.023
	AP2	0.87	0.76	-0.15	0.023
	AP3	0.69	0.48	-0.14	0.02
Passive Resistance	PR1	0.87	0.76	-0.15	0.023
	PR2	0.91	0.83	-0.15	0.023
	PR3	0.94	0.88	-0.15	0.023
Active Resistance	AR1	0.68	0.46	-0.17	0.029
	AR2	0.93	0.86	-0.14	0.02
	AR3	0.75	0.56	-0.14	0.02
Average		**0.79**	**0.64**	**-0.16**	**0.028**

Appendix E – Shortened Survey

Construct	Questions	
Sensitivity of Information	SI1	I do not feel comfortable with the type of information the system requests from me.
	SI2	I feel that the system requests highly sensitive information about me.
	SI3	The information I provide to the system is very sensitive to me.
Perceived Control	PC1	I believe I have control over who can get access to my information requested by the system.
	PC3	I believe I have control over how information is used by the system.
	PC4	I believe I can control my information provided to the system.
Perceived Information-Based Vulnerability (PIBV)	PIBV1	Submitted information could be misused.
	PIBV2	Submitted information could be made available to unknown individuals in my company without my knowledge.
	PIBV3	Submitted information could be inappropriately used.
	PIBV5	It might be beneficial for my company to use submitted information without considering my interests.
	PIBV7	Submitted information could be exploited by the company.
Psychological Contract Breach	PCB1	Almost all the promises made by my employer during recruitment have been kept so far (reverse).
	PCB4	I have not received everything promised to me in exchange for my contributions.
	PCB5	My employer has broken many of its promises to me even though I've upheld my side of the deal.
Psychological Contract Violation	PCV3	I feel that my organization has violated the contract between us.
	PCV4	I feel extremely frustrated by how I have been treated by my organization.
Trust into Employer	T1	I am not sure I fully trust my employer (reverse)
	T2	My employer is open and upfront with me.
	T5	My employer is not always honest and truthful (reverse).
	T7	I can expect my employer to treat me in a consistent and predictable fashion.
Perceived Benefits	B1	Revealing my information in the system helps me to obtain advantages.
	B2	I need to provide my information so I can get exactly what I want from the system.
	B3	I believe that as a result of my information disclosure in the system, I can benefit from a better, customized service.

Construct	Questions	
Intention to Disclose	ID1	Please specify the extent to which you would be willing to reveal your information in the system.
	ID2	How probable would it be that you would disclose information in the system?
Apathy	AP2	I don't care about the system
	AP3	I am not interested into the system
Passive Resistance	PR1	I disagree with the implementation of the system.
	PR2	I perceive the system as a negative change.
Active Resistance	AR1	I will ask others not to use the system.
	AR3	I will point out my negative view regarding the system to others.